ConnectPort® LTS Command Reference

ConnectPort LTS 8, ConnectPort LTS 8 MEI,
ConnectPort LTS 8 W, ConnectPort LTS 8 MEI W,
ConnectPort LTS 16, ConnectPort LTS 16 MEI,
ConnectPort LTS 16 W, ConnectPort LTS 16 MEI W,
ConnectPort LTS 16 MEI 2AC,
ConnectPort LTS 32, ConnectPort LTS 32 MEI,
ConnectPort LTS 32 W, ConnectPort LTS 32 MEI W

90001099_C

© Digi International Inc.2012. All Rights Reserved.
Digi, Digi International, the Digi logo, ConnectPort, XBee, and RealPort are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide.

All other trademarks are the property of their respective owners.
Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International.
Digi provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.
This product could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.

Contents

1. Introduction

This book describes the commands in the command-line interface for several Digi product families, listed below. This chapter provides the following:

- A quick reference showing the commands used to configure features or perform configuration tasks from the command line.
- Basic information that applies to all commands, including navigation and editing keys, displaying online help, abbreviating commands, syntax conventions, and entering special characters in string values.
- How to access the command line.
- How to configure an IP address for a ConnectPort LTS product from the command line, if an address has not already been assigned.
- Information about user models and user permissions in ConnectPort LTS products, and how they affect the commands you can issue.

Products to which this book applies

This manual documents the command-line interface for the ConnectPort LTS Family, which includes these products:

- ConnectPort LTS 8
- ConnectPort LTS 8 MEI
- ConnectPort LTS 8 W
- ConnectPort LTS 8 MEI W
- ConnectPort LTS 16
- ConnectPort LTS 16 MEI
- ConnectPort LTS 16 W
- ConnectPort LTS 16 MEI W
- ConnectPort LTS 16 MEI 2AC
- ConnectPort LTS 32
- ConnectPort LTS 32 MEI
- ConnectPort LTS 32 W
- ConnectPort LTS 32 MEI W

Quick reference for configuring features

The following table shows common features that can be configured from the command line, and the commands used to configure each feature. If you are viewing the PDF file of this document, click the commands in the "Commands" column to go to the command descriptions.

Feature/Task	**Commands**
Alarms	"set alarm".
Autoconnection (automatically connect a user to a server or network device)	"set autoconnect". "set serial". "set tcpserial".
Configuration management/administration	Backup/restore a configuration from a TFTP server on the network: "backup" Update firmware: "boot" Reset configuration to factory defaults: "revert" or "boot action=factory" (see "boot") Reboot the device: "boot"
Display current configuration settings in a device	"show"
Ethernet settings	"set ethernet"
Help on device commands	"help and ?"
Host name for a device (Specify a name for the device)	"set host"
IP address settings	"set network"
Multiple Electrical Interface (MEI)	"set switches"
Point to Point Protocol (PPP)	"set ppp"
Port buffering	"display buffers" "set buffer"
Port profiles: sets of preconfigured serial-port settings for a particular use	"set profile"

Feature/Task	Commands
Python program storage and execution on ConnectPort LTS products	To learn about the Python programming language and writing programs: see the *Digi Python Programming Guide*. To configure Python programs to execute when the Digi device boots: "set python" To manually execute a Python program from the command line: "python"
RealPort (COM port redirection) configuration	"set realport" See also the *RealPort Installation Guide*.
Remote login (rlogin)	"rlogin"
Reverting configuration settings	"revert"
RTS Toggle	"set rtstoggle"
Serial port configuration	Serial port communication options: "set serial" Port profiles: "set profile" RTS Toggle: "set rtstoggle" TCP serial connections: "set tcpserial" UDP serial characteristics: "set udpserial"
Security, users, user access permissions, and user groups	See "User permissions in ConnectPort LTS products" on page 14 for a discussion of how users and access permissions are implemented in Digi Connect products. To create users and change user names: "set user" To control access to inbound ports:"set service" To issue new password to user: "newpass" To set permissions associated with various services and commands: "set permissions" To add or remove user groups, change group configuration attributes, or display group configuration attributes: "set group"
Simple Network Management Protocol (SNMP)	To configure SNMP: "set snmp" To enable/disable SNMP service: "set service"

Feature/Task	Commands
Simple Mail Transfer Protocol (SMTP) settings	To configure SMTP settings: "set smtp"
Set system information: assign system-identifying information to a device	"set system".
Socket tunnel setting	"set socket_tunnel"
Statistics for your ConnectPort LTS product	"info"
Status of your ConnectPort LTS product	"display" "status" "who"
Telnet to network devices	"telnet"
LCD	"set lcd"
NFS	"set nfs"
Samba	"set samba"
SD memory	"set sdmemory"
Syslog	"set syslog"
Trace	"set trace"
USB	"set usb"
Web	"set web"
XBee	"set xbee"

Access the command line

To configure devices using commands, you must first access the command line, and then log on as needed.

This procedure assumes that you have already configured the ConnectPort LTS product with an IP address.

1. To access the command-line interface for the ConnectPort LTS product, enter the following command from a command prompt on another networked device, such as a server:

   ```
   #> telnet   ip address
   Or
   #> ssh user@ ip address
   ```

   Where:

   ip address is the ConnectPort LTS product's IP address.

   user is the username on ConnectPort LTS product.

   For example:

   ```
   #> telnet 192.3.23.5
   Or
   #> ssh root@192.2.23.5
   ```

   Or connect to the serial console port with a terminal emulator.

2. A login prompt is displayed. If you do not know the user name and password for the device, contact the system administrator who configured the device. The default username is "root" and the default password is "dbps."

3. If the system interface access option of the user is set as "Shell", the bash-shell can be accessed after authentication is passed. To access configuration-shell from the bash-shell, enter following command on the bash-shell.

   ```
   #> configshell
   ```

   If the system interface access option of the user is set as "CLI menu", the configuration-shell can be accessed directly after authentication is passed. For details on configuring the system interface access option, see the Digi product's *User's Guide* or the "set user" command.

Configure an IP address

If the device to which you will be issuing commands has not already been assigned an IP address, or if the IP address needs to be modified from its initial configuration, see the Digi product's *User's Guide* for details on configuring an IP address.

Basic command information

Navigation and editing keys

Use the keys listed in the table to navigate the command line and edit commands:

Action	Keys
Move the cursor back one space.	Ctrl+b or Left arrow
Move the cursor forward one space.	Ctrl+f or Right arrow
Delete the character to the left of the cursor.	Ctrl+h or Backspace
Scroll back through commands.	Ctrl+p or Upper arrow
Scroll forward through commands.	Ctrl+n or Lower arrow
Execute the command.	Enter

Displaying online help

Help is available for all commands. The table describes how to access it.

For information on...	Type
All commands	`?` (with no additional options)
A specific command	`help [`*`command`*`] OR [`*`command`*`] ?` **Example:** `help info` **Example:** `info ?` **Example:** `set alarm ?`

Abbreviating commands

All commands can be abbreviated. Simply supply enough letters to uniquely identify the command.

Syntax conventions

Presentation of command syntax in this manual follows these conventions:

- Brackets [ ] surround optional material.
- Braces { } surround entries that require you to chose one of several options, which are separated by the vertical bar, |.
- Non-italicized text indicates literal values, that is, options or values that must be typed exactly as they appear. Yes and no options are examples of literals.
- Italicized text indicates that a type of information is required in that option. For example, *filename* means that the name of a file is required in the option.

Entering special characters in string values

Several commands have options that are string values, for example the "set alarm" command's "match" option and the "set autoconnect" command's "connect_on_string" option.

Escape sequences for special characters

Special characters can be entered in strings using the following escape sequences:

Escape Sequence	**Processed as:**
*	Match any character. This escape sequence is only available on the "set alarm match=string" option.
\a	Alert character.
\b	Backspace character.
\f	Form-feed character.
\n	New-line character.
\r	Carriage-return character.
\s	Acts as a separator between characters. This sequence allows you to enter a string such as "\xB8\s4" where you want the B8 translated as a hexadecimal character separate from the numeric character 4
\t	Horizontal tab character.
\v	Vertical tab character.
\\	Backslash character (\ ).
\x*N*	A hexadecimal number, where *N* is up to 20 hexadecimal digits. For example: \x10\x2
N	An octal byte, where *N* is up to 3 octal digits. For example: \2 or \208

Length limitations for string values

String values for certain command options have specific limitations on the maximum total string value including special characters, and the maximum parsed value (that is, the character-string length when any escape sequences in the string are processed). The option descriptions note these maximum lengths.

Verifying device support for commands

To verify whether a ConnectPort LTS device supports a particular command or command options, and to get the allowed ranges and limits for command options, you can enter several commands. For example:

- "help" displays all supported commands for a device.
- "?" displays all supported commands for a device.
- "set ?" displays the syntax and options for the "set" command. You can use this to determine whether the device includes a particular "set" command variant.
- "help set" displays syntax and options for the "set" command.
- "set serial ?" displays the syntax and options for the "set serial" command.
- "help set serial" displays the syntax and options for the "set serial" command.

Some options may become available in new firmware revisions or before new documentation is released. Some commands relate only to particular features unique to specific Digi products. For example, the "set wlan" command applies only to wireless products. Other commands may have options that are specific to features that are not available on all devices.

User permissions in ConnectPort LTS products

The user model in a ConnectPort LTS product influences the commands that users can issue. ConnectPort LTS supports multiple users.

Multi-user model

- User 1 has a default name of “root.” This user is also known as the administrative user.
- User 1 has default permissions that enables the user to issue all commands.
- Permissions for User 1 can be changed to be less than the default root permissions.
- Additional users may be defined as needed. The “set group” command defines user groups (see "set group").

Increasing security for device users

As needed, you can enforce additional security for device users. For example, you can use the autoconnect feature, where a user is automatically connected to another system without accessing the ConnectPort LTS product’s command line. See the "set autoconnect" command on page 55.

2. Command descriptions

backup

Purpose Saves the device configuration to a TFTP server located on the network or a storage device in the ConnectPort LTS device, or restores the configuration.

Required permissions For products with two or more users, permissions must be set to “set permissions backup=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

```
backup [to=serveripaddress[:filename]|
[to={sd|usb|nfs|samba|userspace}[:filename]]
[from=serveripaddress[:filename] print]|
[from={sd|usb|nfs|samba|userspace}[:filename]]
```

Options

to=*serveripaddress*[:*filename*]

The IP address of the TFTP server to which the configuration will be saved, and the filename that the configuration will be saved as. If a filename is not specified, the default filename of config.rci is used.

to=(sd|usb|nfs|samba|userspace)[:*filename*]

The location of the storage device to which the configuration will be saved, and the filename to which hat the configuration will be saved. If a filename is not specified, the default filename of config.rci is used.

from=s*erveripaddress*[:*filename*]

The IP address of the TFTP server and the filename from which the configuration will be restored. If a filename is not specified, the default filename of config.rci is assumed. In ConnectPort LTS, the system will be rebooted after restoring configuration.

from=(sd|usb|nfs|samba|userspace)[:*filename*]

The location of the storage device and the filename from which the configuration will be restored. If a filename is not specified, the default filename of config.rci is used.

print

Prints out the current device configuration.

Example

```
#> backup from=10.0.0.1:config.rci
```

bash

Purpose Initiates the BASH Linux shell.

Required permissions Root privileges are required to initiate the BASH shell.

Syntax **Initiate BASH shell**

```
bash
```

boot

Purpose

Reboots the ConnectPort LTS product, restores the device configuration to factory default settings, or loads new firmware files from a TFTP server.

Required permissions

For products with two or more users, permissions must be set to “set permissions boot=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

Reboot the ConnectPort LTS product

```
boot action=reset
```

Restore configuration defaults

```
boot action=factory
```

Load new firmware into flash ROM from a TFTP host

```
boot load=host ip address:loadfile
```

Options

action

The action to be performed.

factory

Resets the entire configuration to factory defaults, and then reboots the device.

reset

Reboots the device.

load

The firmware to be loaded.

host ip address

The IP address of a host with new firmware, which is then burned into flash ROM. The host must be running a TFTP server.

loadfile

The name of a firmware file. The software automatically detects the type of file and performs the appropriate load operation.

Examples

Restore configuration defaults

This example reloads the firmware stored in flash ROM and resets the configuration to factory defaults then reboots the device.

```
#> boot action=factory
```

Reboot using the current firmware and configuration

This example reboots the device and uses the current firmware and configuration stored in flash ROM.

```
#> boot action=reset
```

Reboot using firmware from a boot host

This example loads the firmware stored on the TFTP host into flash ROM. A reboot is required to use the new firmware.

```
#> boot load=10.0.0.1:firmware.bin
```

See also

"revert"

close

Purpose

Closes active connect, Rlogin, and Telnet sessions; that is, sessions opened by "connect," "rlogin," or "telnet" commands.

The "close" command is associated with the sessions displayed by the"status" command.

A "close" command issued without any options closes the current connection.

To issue the "close" command, you must first escape the active session. Do this by pressing the escape key defined for your session type. The following table lists default escape keys.

Session Type	Default Escape Keys
Connect	Ctrl+[+Enter
Rlogin	~+Enter
Telnet	Ctrl+]+Enter

For ConnectPort LTS, use the command "z suspend telnet" to escape the active Telnet session instead of "e exit telnet". Using the latter command to exit the Telnet session causes the session to be closed automatically and there will be no session to close using "close" command. See the "telnet" command description for details on connecting and closing Telnet connections.

Syntax

`close [{*|`*`connection number`*`}]`

Options

*****

Closes all active sessions.

connection number

Identifies the session to close by its session number.

Examples

Close a session identified by number

```
#> close 1
```

Close the current session

```
#> close
```

Close all active sessions

```
#> close *
```

See also

• "kill"**.** The kill command has a broader effect than close, and lets you kill connections from the global list. That is, it is not limited to sessions associated with the current connection.

• "status" for information on displaying status information on active sessions.

• "connect"

• "rlogin"

• "telnet"

connect

Purpose

Used to make a connection, or establish a session, with a serial port.

Required permissions

For products with two or more users, permissions must be set to “set permissions connect=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

There are several ways to create and manage connections:

Create a single connection

```
connect serial port
```

Create multiple connections

Issue multiple “connect” commands.

Temporarily suspend a connection

Escape the active session by pressing Ctrl [.

Temporarily suspend a connection and return to the command line

Press the escape character and then the Enter key.

Options

serial port

The number of the port on which to establish a connection.

Example

Create a connection to port 1

```
#> connect 1
```

See also

- "close" for information on ending a session.
- "reconnect" for information on reestablishing a port connection.

display

Purpose

Displays status information for the device. The “display” command’s focus is on real-time information. In contrast, the “info” command displays statistical information about a device over time, while the “status” command displays the status of outgoing connections (connections made by “connect,” “rlogin,” or “telnet” commands). Status information that can be displayed includes:

- General product information, including the product name, MAC address, boot, post, and firmware versions, memory usage, CPU utilization, and uptime, or the amount of time since the device was last booted.
- Access control status information.
- ARP table information.
- Contents of a port buffer (see also "display buffers").
- Serial modem signals (DTR, RTS, CTS, DSR, DCD).
- Socket status information.
- Current TCP and UDP session and listener information.
- Uptime information only.
- Version information for Boot, firmware, and Digi part numbers for those items.

Required permissions

For products with two or more users, permissions must be set to “set permissions display=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

```
display {arp|buffers|device|dnsserver|memory|
  netdevice|proxyarp|serial|sockets|tcp|udp|
  uptime|versions|xbee {refresh|clear}}
```

Options

arp

Displays ARP table entries.

buffers

Displays the contents of a port buffer. This option is covered in more detail in "display buffers".

device

Displays general product information including product name, MAC address, boot, and firmware versions, memory usage, CPU utilization, and uptime. The information displayed by this option is the same as that displayed by the “info device” command (see "info")

dnsserver

Displays DNS server information.

memory

Displays memory usage.

netdevice

Displays the active interfaces on the system, for example, PPP and Ethernet interfaces, and their status, such as “Closed” or “Connected.”

proxyarp

Displays Proxy ARP table entries.

serial

Displays serial modem signals (DTR, RTS, CTS, DSR, DCD).

sockets

Displays information about how socket resources are being used by the system.

tcp

Displays active TCP sessions and active TCP listeners. To display more TCP-related statistics, such as number of input and output bytes transmitted, issue an “info tcp” command (see "info").

udp

Displays current UDP listeners. To display more UDP-related statistics, such as number of input and output bytes transmitted, issue an “info udp” command (see "info").

uptime

Displays amount of time since the device was booted.

versions

Displays boot firmware version information.

xbee {refresh|clear}

Displays or refreshes device information of XBee module on the network. For products with two or more users, permissions must be set to “set permissions s-xbee = read” to user this command. See "set permissions" for details on setting user permissions for commands.

refresh

Refresh the information of XBee devices on the network

clear

Remove current network information of XBee devices and refresh the information of XBee devices on the network again.

Example

Display device information

```
#> display device
device information:

  product           : ConnectPort LTS 32 MEI W
  mac address #1     : 00:40:9D:CC:CC:C6
  mac address #2     : 00:40:9D:56:47:39
  firmware version    : N/A
  bios version       : N/A
  cpu utilization     : 1 %
  uptime            : 2 hours 51 seconds
  total memory       : 255944
  used memory        : 40760
  free memory        : 215184
```

See also

- "info"
- "show"
- "status"

display buffers

Purpose

Displays the contents of a port buffer, or transfers the contents of a port buffer to a server running Trivial File Transfer Protocol (TFTP). Port buffering is enabled by the “set buffer” command (see "set buffer"). Contents are displayed in log form.

Required permissions

For products with two or more users, permissions must be set to one of the following:

- For a user to display the contents of a port buffer for the line on which they are logged in: “set permissions buffers=r-self” or higher.
- For a user to display the contents of a port buffer for any line: “set permissions buffers=read” or higher.

See "set permissions" for details on setting user permissions for commands.

Syntax

```
display buffers [port=range]
  [lines=number][tail=number]
  [tftp=server:filename}]
```

Options

port=*range*

The port or ports to which the command applies. Optional on a single-port device.

lines=*number*

The number of lines of data to display at a time when the “screen” option is specified. Use 0 to indicate continuous flow.

tail=*number*

The total number of lines in the buffer to be displayed. The number is calculated from the end of the buffer counting back.

tftp=*server:filename*

server

The IP address or DNS name of a server running TFTP to which buffer information should be transferred.

filename

The name to use for the file that will be transferred to the TFTP server. If the “port” option specifies more than one port, one file will be transferred for each port. The filename for each port will be “*filename_n*,” where *n* is the port number.

Examples

Display port buffering information on the screen

```
#> display buffers port=2 screen lines=32 tail=30
```

Output buffering information to a TFTP server

```
#> display buffers port=2 tftp=192.168.1.1:port_ouput
```

Output multi-port buffering information to a TFTP server

```
#> display buffers port=2-3 tftp=192.168.1.1:port_ouput
```

Note that port 2 buffering information goes to file port_output_2 and port 3 buffering information goes to file port_output_3.

See also

• "set buffer".

exit

Purpose Terminates the current session.

Syntax `exit`

Example `#> exit`

See also "quit". The “quit” and “exit” commands perform the same operation.

help and ?

Purpose Displays help about a specific command.

Syntax `help [command]`

OR

`[command]?`

Examples

```
#> help boot
#> boot?
#> help set serial
#> set serial?
```

See also "Displaying Online Help"

info

Purpose

Displays statistical information about a device.

The "info" command displays statistical information about a device over time. In contrast, the "display" command's focus is on real-time information, while the "status" command displays the status of outgoing connections (connections made by "connect," "rlogin," or "telnet" commands). Command options allow display of the following categories of statistics:

- Device statistics
- Ethernet statistics
- ICMP statistics
- IP statistics
- Serial statistics
- TCP statistics
- UDP statistics
- Zigbee statistics

The statistics in these tables are those gathered since the tables were last cleared. The statistics tables are cleared by rebooting the ConnectPort LTS product.

Syntax

```
info {device|ethernet|icmp|ip|serial|tcp|
  udp|zigbee_sockets}
```

Options

For a description of the statistics displayed by all these options see the statistics tables in the “Output” section of this description.

device

Displays statistics from the device table. This information includes device-model information, MAC address, current Bios and firmware, memory usage, utilization, and uptime. The information displayed by this option is the same as that displayed by the “display device” command (see "display").

For models with dual power supplies, such as ConnectPort LTS 16 MEI 2AC, this command displays the status of the power supplies (“Normal” or “Fail.”).

ethernet

Displays statistics from the Ethernet table.

icmp

Displays statistics from the ICMP table.

ip

Displays statistics from the IP table.

serial

Displays statistics from the serial table. For descriptions of these statistics, see "Output" section below.

tcp

Displays statistics from the TCP table.

udp

Displays statistics from the UDP table.

zigbee_sockets

Displays statistics from the Zigbee socket information.

Output

Following are descriptions of the statistics displayed for each “info” command option. The statistics displayed include data, event, and error counts. These statistics are useful in understanding how the device is operating and can be helpful in finding problems. In particular if an error counter is found to be increasing you may have a problem with the device. To reset the statistics, reboot the device.

Device statistics

Device Information	Description
Product	The model of the device.
MAC Address #1 & #2	A unique network identifier for Ethernet interface #1 & #2, respectively. All network devices are required to have their own unique MAC address. The MAC address is on a sticker on your device. The number is displayed as 12 hexadecimal digits, usually starting with 00:40:9D.
Firmware Version	The current firmware version. This information may be used to help locate and download new firmware. Firmware updates may be downloaded from the Digi Support website.
Bios Version	The current bios version.
CPU Utilization	The amount of CPU resources being used by the device.
Uptime	The amount of time the device has been running since it was last powered on or rebooted.
Total Memory	The total amount of memory (RAM) available.
Free Memory	The amount of memory (RAM) currently not used.
Used Memory	The amount of memory (RAM) currently in use.

Ethernet statistics

Statistic	Description
InBytes	Number of bytes received.
OutBytes	Number of bytes sent.
InUcastPkts	Number of Unicast packets received.
OutUcastPkts	Number of Unicast packets sent.
InNonUcastPkts	Number of non-Unicast packets received.
InDiscards	Number of incoming packets that were discarded.
OutDiscards	Number of outgoing packets that were discarded.
InErrors	Number of incoming packets that contained errors.
OutErrors	Number of outgoing packets that contained errors.

ICMP statistics

Statistic	Description
InMessages	Number of incoming messages.
OutMessages	Number of outgoing messages.
InDestUnreachables	Number of incoming destination-unreachable messages received. A destination-unreachable message is sent to the originator when a datagram fails to reach its intended destination.
OutDestUnreachables	Number of destination-unreachable messages sent. A destination-unreachable message is sent to the originator when a datagram fails to reach its intended destination.
InErrors	Number of incoming received messages with errors.

IP statistics

Statistic	Description
InReceives	Number of datagrams received.
OutRequests	Number of datagrams given to IP to transmit.
InAddressErrors	Number of received datagrams discarded because they were for another host and could not be forwarded.
DatagramsForwarded	Number of received datagrams forwarded to another host.
InHeaderErrors	Number of received datagrams discarded because of invalid header information.
OutNoRoutes	Number of received datagrams discarded because no route to the destination IP address could be found.
InUnknownProtos	Number of received datagrams discarded because the specified protocol is not available.
OutDiscards	Number of outgoing datagrams that were discarded for miscellaneous reasons. This statistic is not used and is always zero.
InDiscards	Number of received datagrams discarded for miscellaneous reasons.
FragCreates	Number of outgoing datagram fragments created.
ReassembleOks	Number of received datagrams that were successfully reassembled from fragments.
FragOks	Number of outgoing datagrams that were fragmented.
FragFails	Number of outgoing datagram fragmentation attempts that failed. This statistic is not used and is always zero.

Serial statistics

Statistic	Description
rbytes	Total data in: the number of bytes received.
tbytes	Total data out: the number of bytes transmitted.
overrun errors	The number of times FIFO has overrun. The next data character arrived before the hardware could move the previous character.
frame errors	The number of framing errors detected. The received data did not have a valid stop bit.
parity errors	The number of parity errors detected. The received data did not have the correct parity setting.
breaks	The number of break signals detected.

TCP statistics

Statistic	Description
InSegments	Number of segments received.
OutSegments	Number of segments sent.
InErrors	Number of segments received with errors.
RetransmitSegments	Number of segments retransmitted. Segments are retransmitted when the ConnectPort LTS product doesn't respond to a packet sent by the client. This is to handle packets that might get lost or discarded somewhere in the network.
EstabResets	Number of established connections that have been reset.
OutResets	Number of outgoing connections that have been reset.
PassiveOpens	Number of passive opens. In a passive open, the ConnectPort LTS product is listening for a connection request from a client.
ActiveOpens	Number of active opens. In an active open, the ConnectPort LTS product is initiating a connection request with a server.
Established	Number of established connections.
Attempt Fails	Number of failed connection attempts.

UDP statistics

Statistic	Description
InDatagrams	Number of datagrams received.
OutDatagrams	Number of datagrams sent.
InErrors	Number of bad datagrams that were received. This number does not include the value contained by "No Ports"
NoPorts	Number of received datagrams that were discarded because the specified port was invalid.

ZigBee socket statistics

Statistic	Description
Frames Sent	Number of frame sent.
Frames Received	Number of frame received.
Transmit Frame Errors	Number of bad frame that were sent.
Receive Frame Errors	Number of bad frame that were received.
Bytes Sent	Number of byte sent.
Bytes Received	Number of byte received.
Receive Bytes Droppred	Number of received byte that were dropped due to an exhaustion of internal buffers.
Receive Bytes Truncated	Number of received byte that were dropped because the user buffer passed to recvfrom() was not large enough to contain the entire packet.

Example **Display ICMP statistics**

```
#> info icmp
ICMP statistics:

InMessages            : 3         OutMessages         : 5
InDestUnreachables    : 2         OutDestUnreachables   : 2
InErrors              : 0

ICMPv6 statistics:

InMessages            : 0        OutMessages          : 11
InDestUnreachables    : 0      OutDestUnreachables   : 0
InErrors              : 0
```

See also

- "display" .
- "show".
- "status"

kill

Purpose

Kills or ends connections. The “kill” command is associated with the connections displayed by the “who” command.

RealPort sessions cannot be killed by this command.

Required permissions

For products with two or more users, permissions must be set to “set permissions kill=execute” to use this command.
See "set permissions" for details on setting user permissions for commands.

Syntax

`kill [range] [connection id]`

Options

range

A range of connection IDs.

connection id

An ID for the connection.

Examples

Killing a session on a specific port

```
#> kill 1
```

Killing a session on a range of ports

```
#> kill 1-3
```

newpass

Purpose Creates or changes user passwords for the device.

Required permissions For products with two or more users, permissions must be set to “set permissions newpass=rw-self” for a user to set their own password, and “set permissions newpass=rw” to set another user’s password. See "set permissions" for details on setting user permissions for commands.

Syntax `newpass [{id=number|name=string}]`

Options

id=*number*

Specifies the ID of the user to be acted on.

name=*string*

Specifies the name of the user to be acted on.

Examples The “newpass” command initiates a dialog that changes the user’s password.

User changing their own password

```
#> newpass
```

Changing another user’s password

```
#> newpass name=jdoe
```

See also

- "set user" for information on configuring users.
- **“**User permissions in ConnectPort LTS products” on page 14

ping

Purpose

Tests whether a host or other device is active and reachable. To interrupt the "ping" command, use Ctrl-C.

Required permissions

For products with two or more users, permissions must be set to "set permissions ping=execute" for a user to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

`ping` *`ipaddress`* `[`*`options`*`]`

Options

ipaddress

Identifies the target of the "ping" command by its IP address.

options

The options associated with the "ping" command, which are:

count=0|*n*

The number of "ping" commands to be issued. 0 means ping until interrupted. The default is 0.

size=*bytes*

The number of bytes to send in each ping packet. The default is 56 bytes.

version=v4|v6

The Internet protocol version of ping packet. The default is v4.

iface=*interface name or ip address as source*

The interface name or IP address that will be used as source of ping packet. The default is eth0.

Example

Specify a simple ping

The following command determines whether the specified host can be reached:

```
#> ping 199.150.150.10
```

python

Purpose

Manually executes a Python program from the command line. The “python” command is similar to a command executed on a PC. However, other than a program name and arguments for the program, the command takes no arguments itself, and is currently unable to spawn an interactive session.

Syntax

```
python [tftp server ip address:]filename
  [program arguments...]
```

Options

[(*tftp server ip address*):]*filename*

The main file to be executed. This file can be either a file on the file system accessed through the Web UI, or a file accessible through a TFTP server on the network. This TFTP functionality reduces the number of times that you may need to place a program on the file system while developing and refining functionality. However, the TFTP behavior only works for the main program. Modules and packages must still be present on the file system to be used.

program arguments...

Arguments to be supplied to the program.

See also

• "set python" to manually execute a Python program.

• *The Digi Python Programming Guide* to learn more about the Python programming language as implemented in Digi products, and writing Python programs.

quit

Purpose	Use the quit command to log out of the device.
Syntax	`quit`
Example	`#> quit`
See also	"exit". The “quit” and “exit” commands perform the same operation.

reconnect

Purpose

Reestablishes a previously established connection; that is, a connection opened by a “connect,” “rlogin,” or “telnet” command. The default operation of this command is to reconnect to the last active session.

Required permissions

For products with two or more users, permissions must be set to “set permissions reconnect=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

```
reconnect [{serial port|
  p=serial port|s=session}]
```

Options

serial port

The serial port to which this command applies. Use this option to reconnect to a session opened by a connect command.

p=*serial port* | s=*session*

The serial port number or session number (displayed by the “status” command) to reconnect to. In case of serial port, the session order to reconnect is current active session and then small session id if there are two or more sessions for a serial port and user specify “p=serial port” option to reconnect.

Examples

Reconnect to the last port used

```
#> reconnect
```

Reconnect to port 1

```
#> reconnect p=1
```

Reconnect to session 1

```
#> reconnect s=1
```

See also

- "connect" for information on establishing a connection on a selected port.
- "close" for information on ending a connection.
- "status" for information on gathering status on current connections.
- "rlogin"
- "telnet"

revert

Purpose

Reverts all or a subset of a devices' configuration settings to their default values. If you enter "revert user," "revert group," or "revert permissions," a message is displayed indicating that those settings cannot be reverted individually, and instead must be reverted all together at the same time via the "revert auth" command. The "revert auth" command (revert authentication and authorization) reverts all users, all groups, and all permissions at the same time.

Required permissions

No "set permissions" option is required for all "revert" command variants except "revert all." The permissions used by the various "set" commands apply to the various "revert" command variants. "revert all" uses a different mechanism that bypasses the individual "set" commands, and therefore has its own permissions. To execute the "revert all" command, a user must have permissions set to "set permissions revert-all=execute". See "set permissions" for details on setting user permissions for commands.

Syntax

```
revert [all|
  alarm|
  auth [uid=range][gid=range]|
  autoconnect [port=range]|
  buffer [port=range]|
  host|
  lcd|
  modem [port=range]|
  network|
  nfs|
  pmodem [port=range]|
  portauth [port=range]
  portgroup|
  ppp|
  profile [port=range]|
  python|
  realport|
  rtstoggle [port=rtstoggle]|
  samba|
  sdmemory|
  serial [port=range]|
  serialport [port=range]
  service|
  smtp|
  snmp|
  socket_tunnel|
  switches [port=range]|
  sysauth|
  syslog|
  system|
  tcpserial [port=range]|
  udpserial [port=range]|
  usb|
  web|
  xbee]
```

Options

all

Reverts all settings except network settings, security settings (passwords and suppress login), and host key settings.

alarm

Reverts the alarm settings configured by the “set alarm” command.

auth [uid=*range*] [gid=*range*]

Reverts the permission settings configured by the “set permissions” command, the user settings configured by the “set user” command, and group settings, configured by the “set group” command.

autoconnect [port=*range*]

Reverts the autoconnect settings configured by the “set autoconnect” command.

buffer [port=*range*]

Reverts the port-buffering settings configured by the “set buffer” command.

host

Reverts the host name set by the “set host” command.

lcd

Reverts the host name set by the “set lcd” command.

modem [port=*range*]

Reverts the host name set by the “set modem” command.

network

Reverts the network settings, configured by the “set network” command.

nfs

Reverts the NFS settings, configured by the “set nfs” command.

pmodem [port=*range*]

Reverts the modem emulation settings, configured by the “set pmodem” command.

portauth [port=*range*]

Reverts the Port Authentication settings configured by the “set portauth” command.

ppp

Reverts the Point-to-Point Protocol (PPP) settings, configured by the “set ppp” command.

profile [port=*range*]

Reverts the profile settings configured by the “set profile” command.

python

Reverts the Python program settings configured by the "set_python" command.

realport

Reverts the Realport settings configured by the “set realport” command.

rtstoggle [port=*range*]

Reverts the Rtstoggle settings configured by the “set rtstoggle” command

samba

Reverts the service settings configured by the “set samba” command.

sdmemory

Reverts the SD memory settings configured by the “set sdmemory” command.

serial [port=*range*]

Reverts the serial settings configured by the “set serial” command.

serialport [port=*range*]

Reverts all serial settings configured by the “set serial”, “set tcpserial”, “set udpserial”, “set profile”, “set serial”, “set buffers”, “set pmode”, and “set modem” command.

service

Reverts the service settings configured by the “set service” command.

smtp

Reverts the SMTP settings configured by the “set smtp” command.

snmp

Reverts the SNMP settings configured by the “set snmp” command.

socket_tunnel

Reverts the socket tunnel settings configured by the “set socket_tunnel” command.

switches [port=*range*]

Reverts the switch settings configured by the “set switches” command.

syslog

Reverts the SYSLOG settings configured by the “set syslog” command.

system

Reverts the system settings configured by the “set system” command.

tcpserial [port=*range*]

Reverts the TCP serial settings configured by the “set tcpserial” command.

udpserial [port=*range*]

Reverts the UDP serial settings configured by the “set udpserial” command.

usb

Reverts the USB settings configured by the “set usb” command.

web

Reverts the Web settings configured by the “set web” command.

xbee

Reverts the XBee settings configured by the “set xbee” command.

Examples

Reset a device’s serial setting

The device serial setting is reset to the default serial configuration.

```
#> revert serial
```

Reset a serial port to default settings

```
#> revert serial port=2
```

See also

- "boot"
- The various “set” commands referenced in this description.
- "show"

rlogin

Purpose

Performs a login to a remote system, also referred to as an rlogin.

Required permissions

For products with two or more users, permissions must be set to “set permissions rlogin=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

```
rlogin [esc=character]
  [{user=username}]
  [ip address]
```

Options

esc= character

A different escape character than the ~ (tilde) character, which will be used for the current Rlogin session. This character is used for suspending a session from the remote host to return to the device server command line.

user=*username*

The user name to use on the remote system. If you do not specify a name, your device server user name will be used.

ip address

The IP address of the system to which you are performing the remote login.

Example

```
#> rlogin 10.0.0.1
```

See also

- "telnet"
- "connect"
- "status"
- "close"

set alarm

Purpose

Configures device alarms and display current alarm settings. Device alarms are used to send emails or SNMP traps when certain device events occur. These events include data patterns detected in the serial stream.

To avoid false errors, configure alarms while alarms are disabled, by entering a "set alarm state=off" command, then enable alarms after they are fully configured by entering "set alarm state=on".

Required permissions

For products with two or more users, permissions must be set to "set permissions s-alarm=read" to display current alarm settings, and to "set permissions s-alarm=rw" to display alarm settings and configure alarms. See "set permissions" for details on setting user permissions for commands.

Syntax

Configure alarms with general options (applies to all alarms)

```
set alarm [state={on|off}]
```

Configure alarms for a range (set multiple alarms)

```
set alarm range={1-32}
  [active={on|off}|to=string|cc=string|subject=string
  |priority={normal|high}|type={email|snmptrap|all}]
```

Configure alarms based on data pattern matching

```
set alarm port=1-16
  match=string
```

Display current alarm settings

```
set alarm [range={1-32}]
```

Options

General alarm options

state= {on|off}

Enables or disables all alarms.

on

Enables all alarms.

off

Disables all alarms. To avoid false errors, it is recommended that you configure alarms while alarms are disabled, and enable alarms after they are fully configured.

The default is “off.”

Options for setting multiple alarms with the “range” option

range= {1-32}

Specifies the alarm or range of alarms for which alarm options are set.

active={on|off}

Enables or disables an alarm.

on

Enables an alarm.

off

Enables an alarm.

The default is “off.”

cc=*string*

The text to be included in the “cc” field of an alarm-triggered email.

priority={normal|high}

The priority of the triggered email.

normal

The email is sent with normal priority.

high

The email is sent with high priority.

The default is “normal.”

subject=*string*

If “type=email,” this option specifies the text to be included in the “subject” field of an alarm-triggered email. If “type=snmptrap,” this option specifies the text to be included in the “Serial Alarm Subject” field of an alarm-triggered SNMP trap.

to=*string*

The text to be included in the “to” field of an alarm-triggered email.

type={email|snmptrap|all}

Used to determine what kind of an alarm is sent: an e-mail alarm, an SNMP trap or both.

For SNMP traps to be sent, the IP address of the system to which traps are sent must be configured, by issuing a “set snmp” command with the “trapdestip” option. See "set snmp."

email

An email alarm is sent.

snmptrap

An SNMP trap is sent. If snmptrap is specified, the “subject” text is sent with the alarm. The MIBs for these traps are DIGI-SERIAL-ALARM-TRAPS.mib, and DIGI-MOBILETRAPS.mib.

all

Both an email alarm and SNMP trap are sent.

The default is “email.”

Data pattern matching-based alarm options

In data pattern match mode, an alarm will be triggered when a pattern is found in the stream of serial data. These options are used for setting alarms in data pattern match mode:

port=1-16

The serial ports to which the data pattern match alarm applies.

match=*string*

A string that triggers an alarm if the data pattern is found in the incoming serial stream. The maximum length of this string is 32 characters, including escape sequences for special characters. For more details on the escape sequences, see "Entering Special Characters in String Values". The maximum parsed length of this string is 10 characters. That is, this string must reduce down to a 10-character string when the escape sequences are processed.

Examples

Set alarms based on data pattern matching

This command turns on alarm 10, and sends the alarm via snmptrap. The snmptrap is sent if the pattern “failure” is seen on port 5. The trap title will display as “failure alarm.”

```
#> set alarm range=10 active=on type=snmptrap
match="failure" subject="failure alarm" port=5
```

This command turns on alarm 11, and sends the alarm via email. The email is sent to fred@digi.com , with “Email alarm” on the subject line with a high priority. An alarm is sent if port 16 shows “kernel failure” pattern.

```
#> set alarm range=11 active=on type=email
to=fred@digi.com subject="Email alarm" priority=high
match="kernel failure" port=16
```

set autoconnect

Purpose

Used to establish an automatic connection (autoconnection) between the serial port and a remote network destination, and to display current autoconnect settings.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display autoconnect settings for the line on which they are logged in: “set permissions s-autoconnect=r-self”
- For a user to display autoconnect settings for any line: “set permissions s-autoconnect=read”
- For a user to display and set the autoconnect settings for the line on which they are logged in: “set permissions s-autoconnect=rw-self”
- For a user to display autoconnect settings for any line, and set the autoconnect settings for the line on which the user is logged in: “set permissions s-autoconnect=w-self-r”
- For a user to display and set the autoconnect settings on any line: “set permissions s-autoconnect=rw” See "set permissions" for details on setting user permissions for commands.

Syntax

Configure autoconnect

```
set autoconnect
  [port={range|xbee|internalmodem}]
  [state={on|off}]
  [trigger={always|data|dcd|dsr|string}]
  [service={raw|rlogin|ssl|telnet|ssh}]
  [description=string]
  [ipaddress=ip address]
  [ipport=ip port]
  [connect_on_string=string]
  [flush_string={on|off}]
  [keepalive={on|off}]
  [nodelay=on|off]
```

Display autoconnect settings

```
set autoconnect [port={range|xbee|internalmodem}]
```

Options

port={range|xbee|internalmodem}

Used to specify the serial port. Optional on a single-port device.

To configure settings for the XBee port, specify “port=xbee.”And to configure settings for an internal modem port, specify “port=internalmodem.”

state={on|off}

Enables or disables the autoconnect feature.

on

Enables the autoconnect feature.

off

Disables the autoconnect feature.

The default is off.

If you are using the serial port for another purpose, it is recommended this value be set to “off.”

trigger={always|data|dcd|dsr|string}

Indicates which events from the serial port will trigger a network connection to occur.

always

The serial port will continually attempt to keep a connection to a remote network destination active.

data

The serial port will attempt a network connection whenever data arrives on the serial port.

dcd

The serial port will attempt a network connection whenever the serial port's DCD signal goes high.

dsr

The serial port will attempt a network connection whenever the serial port's DSR signal goes high.

string

A connection will be made upon detecting a particular sting, specified by the "connect_on_string" option, in the data from the serial port.

The default is "always."

service={raw|rlogin|ssl|telnet|ssh}

The type of network connection that will be established.

raw

A connection without any special processing will occur.

rlogin

A remote login (rlogin) connection will occur.

ssl

A secure connection conforming to SSL (Secure Sockets Layer) Version 3 and Transport Layer Security (TLS) Version 1 will occur.

telnet

A connection with Telnet processing will occur.

ssh

A SSH(Secure Shell) connection will occur. The default is "raw."

description=*string*

A name for descriptive purposes only.

ipaddress=*ip address*

The IP address of the network destination to which a connection will be made.

ipport=*ip port*

The TCP port of the network destination to which a connection will be made.

connect_on_string=*string*

When the value of the “trigger” option is string, this option specifies the string that must be found in the serial data in order for a connection to occur. The maximum length of this string is 32 characters, including escape sequences for special characters. For more details on the escape sequences, see "Entering Special Characters in String Values". The maximum parsed length of this string is 32 characters. That is, this string must reduce down to a 32-character string when the escape sequences are processed.

flush_string={on|off}

Indicates whether the connect string, specified by the “connect_on_string” option, is flushed or sent over the newly established connection.

on

The connect string is flushed.

off

The connect string is sent over the newly established connection.

The default is “on.”

keepalive={on|off}

Indicates whether or not TCP keepalives are sent for the specified range of clients. If set to on, keepalives are sent, if it is off, keepalives are not sent. Configurable TCP keepalive parameters, for example, how many keepalives to send and when to send them, are configured globally via the “set network” command (see "set network").

nodelay={on|off}

Used to allow unacknowledged or smaller than maximum segment sized data to be sent.

Note: The “nodelay” option disables Nagle’s algorithm, which is on by default for some TCP services. Nagle's algorithm reduces the number of small packets sent. It instructs to hold on to outgoing data when there is either unacknowledged sent data or there is less than maximum segment size (typically around 1500 bytes for Ethernet) worth of data to be sent. While this algorithm keeps transmission efficient, there are times when disabling it is desirable.

Examples

Set autoconnect on with trigger

This example shows setting autoconnect to connect to the TCP port (2101) of the network IP destination when data arrives on the serial port.

```
#> set autoconnect state=on trigger=data
ipaddress=10.0.0.1 ipport=2101
```

Allow outgoing data that is either unacknowledged or less than maximum segment size

```
#> set autoconnect port=1 nodelay=on
```

See also

- "revert"
- "set network"
- "set serial"
- "set tcpserial"
- "show"

set buffer

Purpose

Configures buffering settings on a port, or displays the port buffer configuration settings on all ports. The port buffering feature allows you to monitor incoming ASCII serial data in log form.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the port buffering settings for the line on which they are logged in: “set permissions buffers=r-self”
- For a user to display the port buffering settings for any line: “set permissions buffers=read”
- For a user to display and set the port buffering settings for the line on which they are logged in: “set permissions buffers=rw-self”
- For a user to display the port buffering settings for any line, and set port buffering settings for the line on which the user is logged in: “set permissions buffers=w-self-r”
- For a user to display and set the port buffering settings on any line “set permissions buffers=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Configure port buffering

```
set buffer [clear] [clearbk]
  [port={range|xbee|internalmodem}]
  [size=number]
  [state={on|off|pause}]
  [autobk=(none|nfs|samba|sdmemory|usb)]
  [autobk_size=0-64]
  [syslog_state={off|on}]
```

Display port buffering settings

```
set buffer [port=port]
```

Options

clear

Clears the contents of the specified buffer.

clearbk

Clears the autobackup file

port

The port or ports to which the command applies. To configure settings for the XBee port, specify port=xbee. And to configure settings for an internal modem port, specify "port=internalmodem."

size

The size in kilobytes to configure the buffer. Settings are configurable in 2-kilobyte increments. The maximum size is 64 kilobytes. The default is 32 kilobytes.

state

The buffering state, which can be any of the following:

on

The data will be buffered.

off

The data will not be buffered and all data will be cleared from the buffer.

pause

The data will not be buffered, but data in the buffer will not be cleared.

autobk

Automatic data backup option. The data will be buffered on following storage location.

none

Automatic data backup will not be enabled.

nfs

The data will be buffered on NFS server.

samba

The data will be buffered on Samba server.

sdmemory

The data will be buffered on SD memory.

usb

The data will be buffered on USB storage device.

autobk_size

The buffer size for automatic data backup option.

syslog_state

The data will be sent to SYSLOG server. To configure SYSLOG server, see “set syslog” command.

on

The data will be sent to SYSLOG server.

off

The data will not be send to SYSLOG server.

Examples

Display port buffer configuration for all ports

```
#> set buffer
```

Configure buffers

In this example, the set buffer command sets the buffer state for port 1 to on mode and the buffer size to 64 kilobytes.

```
#> set buffer port=1 state=on size=64
```

In this example, the set buffer command sets the buffer state for port 1 to on mode and the data will be buffered on NFS server with 16 kilobytes of buffer size.

```
#> set buffer port=1state=on autobk=nfs autobk_size=16
```

In this example, the set buffer command sets the buffer state for port 1 to on mode and the data will be sent to SYSLOG server.

```
#> set buffer port=1state=on syslog_state=on
```

See also

- "revert"
- "show"
- "set syslog"
- "set nfs"
- "set samba"
- "set sdmemory"
- "set usb"
- "set syslog"

set ethernet

Purpose

Configures, adjusts, and displays Ethernet communications options.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-ethernet=read” to display Ethernet communications options, and “set permissions s-ethernet=rw” to display and configure Ethernet communications options. See "set permissions" for details on setting user permissions for commands.

Syntax

Configure Ethernet communications options

```
set ethernet [index=1-2]
  [duplex={half|full|auto}]
  [speed={10|100|1000|auto}]
```

Display Ethernet communications options

```
set ethernet
```

Options

index=1-2

Used to specify the index of the Ethernet device

duplex

Determines the mode the ConnectPort LTS product uses to communicate on the Ethernet network. Specify one of the following:

half

The device communicates in half-duplex mode.

full

The device communicates in full-duplex mode.

auto

The device senses the mode used on the network and adjusts automatically.

The default is “auto.” If one side of the Ethernet connection uses auto, the other side can set the duplex value to whatever is desired. If one side uses a fixed value (for example, half-duplex), the other side has to use the same. If the “speed” value is set to auto, auto is only allowed for the duplex value.

speed={10|100|1000|auto

Configures the Ethernet speed the ConnectPort LTS product will use on the Ethernet network. Specify an appropriate setting for your Ethernet network, which can be one of the following:

10

The device operates at 10 megabits per second (Mbps) only.

100

The device operates at 100 Mbps only.

1000

The device operates at 1000 Mbps only.

auto

The device senses the Ethernet speed of the network and adjusts automatically.

The default is “auto.” If one side of the Ethernet connection is using auto (negotiating), the other side can set the Ethernet speed to whatever value is desired. Or, if the other side is set for 100 Mbps, this side must use 100 Mbps.

Example

Configure 100 Mbps Ethernet speed

```
#> set ethernet speed=100
```

See also

- "set network" to configure network communications options.
- "revert"
- "show"

set group

Purpose

Used to create and manage user groups. You can use “set group” to do the following:

- Add a group. A maximum of 32 groups can be defined.
- Remove groups.
- Change group configuration attributes.
- Display group configuration attributes.

To apply a common set of user settings to more than one user, it may be desirable to create a group with the required settings and then associate that group with multiple users. If a user is a member of one or more groups, the user's effective permissions are the maximum of the permissions of the user and all of the groups to which the user belongs.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-group=read” to display group configuration attributes, and “set permissions s-group=rw” to display and set group configuration attributes. See "set permissions" for details on setting user permissions for commands.

Syntax

Add a group

```
set group add id=number newname=string
```

Remove a group

```
set group remove {id=range|name=string}
```

Change group configuration attributes

```
set group {id=range|name=string} [newname=string]
```

Display group configuration attributes

```
set group {id=range|name=string}
```

Display group configuration attributes for all groups

```
set group
```

Options

add

Add a group. New groups are created with no permissions. A maximum of 32 groups can be defined.

remove

Remove groups.

id=*range*

Specifies the ID or range of IDs of the groups to be acted on.

name= *string*

Specifies the name of the group to be acted on.

newname=*string*

Specifies a new group name.

Default permissions

When a new group is created, it has no permissions.

Examples

Add a new group

```
#> set group add newname=gurus id=4
```

Remove group 7

```
#> set group remove id=7
```

Set a new group name

```
#> set group id=4 newname=gurus
```

See also

- "newpass"
- "revert"
- "set permissions"
- "set user"
- "show"
- “User permissions in ConnectPort LTS products” on page 14

set host

Purpose

Configures a name for the device, also known as a host name, or displays the current host name for the device.

Required permissions

For products with two or more users, permissions must be set to "set permissions s-host=read" to display the current host name, and "set permissions s-host=rw" to display and set the host name. See "set permissions" for details on setting user permissions for commands.

Syntax

Configure a host name for the device

```
set host name=name
```

Display the current host name

```
set host
```

Options

name=*name*

The name for the device. The name can be up to 32 characters long, and can contain any alphanumeric characters, and can also include the underscore (_) and hyphen (-) characters. To enter a multiple-word name with spaces, enclose the name in quotation marks, as shown in the example below.

Examples

```
#> set host name=CPLTS
#> set host name="CPLTS DIGI"
```

See also

"show"

set ippool

Purpose

Creates a pool of IP addresses for serial ports and internal modem, or displays the currently defined pool of IP addresses. This command can be used for configuring IP addresses for PPP connections.

Required permissions

Permissions must be set to “set permissions s-ppp=read” to display ippool configuration settings, and “set permissions s-ppp=rw” to display and set ippool configuration settings. See "set permissions" on for details on setting user permissions for commands.

Syntax

Change ippool configuration settings

```
set ippool [state={off|on}]
  [count=1-32]
  [ip=ip address]
```

Display current ippool settings

```
set ippool
```

Options

state={on|off}

Specifies whether the ippool will be enabled

on

Enable the ippool.

off

Disable the ippool.

count=1-32

Specifies the number of IP address in the pool. Maximum number of IP address in the pool is 32.

ip=*ip address*

The first IP address in the pool.

Example

Specify 32 IP address pools

```
#>set ippool state=on count=32 ip=192.168.100.1
```

See also

• "set ppp"

set lcd

Purpose Configure LCD device settings and displays current LCD settings

Required permissions Permissions must be set to one of the following:

- For a user to display the LCD settings: “set permissions s-lcd=read”
- For a user to display and set the LCD settings: “set permissions s-lcd=rw”

Syntax

Enable/Disable LCD

```
set lcd state=[on|off]
```

Change background image idle time-out

```
set lcd wait_time=wait time
```

Change default background image

```
set lcd use_defaultimage=[on|off]
```

Load background image from tftp server

```
set lcd load_image=host:filename
```

Change the status of backlight

```
set lcd backlight =[on|off]
```

Options

state={on|off}

Sets whether the LCD is enabled or disabled.

on

Enable the LCD display.

off

Disable the LCD display.

wait_time=*wait time*

Specifies the idle time out of LCD background image. When there is no input from LCD key pad during wait time, LCD displays a background image automatically.

use_defaultimage={on|off}

Specifies whether the default background image will be used on idle time out.

on

Use the default background image

off

Use the custom background image loaded by user.

load_image=*host*:*filename*

Specifies the tftp server and file name to be used to upload user custom LCD background image.

host

The IP address or DNS name of a host from which the custom LCD background image will be downloaded to the ConnectPort LTS device using TFTP.

filename

The name of a file on the host that contains the custom LCD background image. If your host's implementation requires a complete path to this file, specify the path here as well. (Be sure that ConnectPort LTS supports only 128x64 8bit bitmap file for LCD background image.)

backlight={on|off}

Specifies the status of LCD backlight.

on

Turn on the LCD backlight.

off

Turn off the LCD backlight.

Examples

Enable LCD display

```
#>set lcd state=on
```

Change background image idle time-out

```
#>set lcd wait_time=30
```

Load a custom LCD background image from TFTP server

```
#>set lcd load_image=192.168.100.1:custom_image
```

See also

• show lcd"

• The *ConnectPort LTS User's Guide's* chapter on the LCD interface.

set modem

Purpose

Used to configure options of modem profile for a serial port, or display current modem profile settings for a serial port.

Required permissions

Permissions must be set to one of the following:

- For a user to display the modem settings: “set permissions s-modem=read”
- For a user to display and set the modem settings: “set permissions s-modem=rw”

Syntax

Configure modem settings

```
set modem [port={1-32|internalmodem}]
  [state={off|on}]
  [connection_type={incoming|outgoing|
    network_bridge}]
  [ppp_connection ={off|on}]
  [init_string=string]
```

Options

port={1-32|internalmodem}

Used to specify the serial port. Optional on a single-port device. To configure settings for an internal modem port, specify “port=internalmodem”.

state={on|off}

Specifies whether the modem will be enabled

on

Enable the modem for a serial port.

off

Disable the modem for a serial port.

connection_type={incoming|outgoing|network_bridge}

Specifies the connection type of a modem profile.

incoming

Used for dial-in connections, such as inbound PPP connections or to manage a device through a telephone network. The ConnectPort LTS product server will receive connections from other hosts.

outgoing

The modem will dial-out to establish connections with external hosts or to connect to an external PPP network.

network_bridge

The modem can be used both to establish connections to other hosts as well as receive connections from other hosts.

ppp_connection={on|off}

Specifies whether the modem will use the PPP connection.

on

Allow user to use the PPP connection.

off

Do not allow user to use the PPP connection.

init_string=*string*

An AT command that is sent to the modem after it is reset.

Examples

Set a serial port to an incoming modem profile

```
#>set modem port=1 state=on connection_type=incoming
```

Display current modem settings

```
#>set modem
```

See also

- "show modem"
- "set ppp"

set network

Purpose Sets and displays network configuration options.

Required permissions For products with two or more users, permissions must be set to "set permissions s-network=read" to display network configuration attributes, and "set permissions s-network=rw" to display and set network configuration attributes. See "set permissions" for details on setting user permissions for commands.

Syntax **Set network configuration options**

```
set network [index=1-4]
  [ipv4 address options]
  [ipv6 address options]
  [dns options]
  [tcp keepalive options]
  [advanced ip options]
```

Where:

[*ipv4 address options*] are:

```
  [mode_v4={none|static|dhcp}]
  [ip_v4=device ipv4 address]
  [submask_v4=subnet mask for ipv4 address]
  [gateway_v4=gateway ipv4 address]
```

[*ipv6 address options*] are:

```
  [mode_v6={none|static|dhcp|auto}]
  [ip_v6=device ipv6 address]
  [gateway_v6=gateway ipv6 address]
  [ip_6to4tunnel={off|on}]
  [ip_v4_6to4relay=ipv4 address of remote
  6to4 relay]
  [ip_v6_v4addr=public ipv4 address for
  6to4 tunneling]
```

[*dns options*] are:

```
  [manual_dns={off|on }]
  [dns1=primary dns server ip address]
  [dns2=secondary dns server ip address]
```

[*tcp keepalive options*] are:
  [idle=10-86400] (seconds)
  [probe_count=5-30]
  [probe_interval=10-75] (seconds)

[*advanced ip options*] are:
  [reuse_old_op={off|on}]
  [autoip={off|on}]
  [sbr={off|on}]

Display current network configuration options

```
set network
```

Options

index=1-4

Select index for Ethernet interface to configure. "index=1" is for setting Ethernet interface 1(eth0) and "index=2" is for setting Ethernet interface 2(eth1). "index=3" and "index=4" are reserved for future use.

[*ipv4 address options*]

Set IP v4 address-related options for the ConnectPort LTS product, including:

mode_v4={none|static|dhcp}

Sets the mode of device IP v4 address

none

Disable IPv4 address.

static

When selected, the device uses the specified IP address, gateway address, and subnet mask.

dhcp

When selected, the device attempts to use the DHCP protocol to find an IP address, gateway address, and submask.

Default is "static" for Ethernet interface 1 and "none" for Ethernet interface 2.

ip_v4=*device ipv4 address*

Sets the device IP v4 address when DHCP is off. This option is only applicable if the “mode_v4” option is set to “static”

submask_v4= *subnet mask for ipv4 address*

Sets the device submask address when DHCP is off. This option is only applicable if the “mode_v4” option is set to “static”

gateway_v4= *gateway ipv4 address*

Sets the network gateway IP address.

[*ipv6 address options*]

Set IPv6 address-related options for the ConnectPort LTS product, including:

mode_v6={none|static|dhcp|auto}

Sets the mode of device IP v6 address

none

Disable IPv6 address.

static

When selected, the device uses the specified IP address and gateway address.

dhcp

When selected, the device attempts to use the DHCP v6 protocol to find an IP address and gateway address.

auto

When selected, the device attempts to use the stateless autoconfiguration protocol to find an IP address and gateway address.

Default is “none” for both Ethernet interface 1 and 2.

ip_v6= *gateway ipv6 address*

Sets the device IP v6 address when DHCP or Auto configuration is off. This option is only applicable if the “mode_v6” option is set to “static.”

gateway_v6= *gateway ipv6 address*

Sets the network gateway IP address.

ip_6to4tunnel={off|on}

Set this option on to supply 6to4 Tunneling which consists of encapsulating IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6 so that ConnectPort LTS product can reach the remote IPv6 Internet through the existing IPv4 infrastructure.

on

Enable 6to4 Tunneling

off

Disable 6to4 Tunneling.

ip_v4_6to4relay= *ipv4 address of remote 6to4 relay*

Set the IPv4 address of the remote 6to4 relay device.

ip_v6_v4addr= *public ipv4 address for 6to4 tunneling*

Set the public IPv4 address to be used for 6to4 tunneling. If not set, current IPv4 address of ConnectPort LTS will be used.

[*dns options*]

Set DNS(Domain Name Server)-related options for the ConnectPort LTS product, including:

manual_dns={off|on }

Configure manual DNS(Domain Name Server) option for the ConnectPort LTS product

on

Enable manual DNS.

off

Disable manual DNS.

dns1=*primary dns server ip address*

dns2=*secondary dns server ip address*

For DNS, these options specify the DNS nameservers to use. Name lookups will be performed using the nameserver specified on “dns1” first, and if fails, the nameserver specified on “dns2” will be used.

[*tcp keepalive options*]

Are options that configure how TCP keep-alive probes are sent. The keep-alive options (“idle,” “probe_count,” “probe_interval”) should be configured for various services that are configured by “set service keepalive={on|off},” or clients such as autoconnect (“set autoconnect keepalive={on|off}”).

idle=10-86400

The amount of time, in seconds, to wait while not receiving TCP packets before sending out a keep-alive probe.

probe_count=5-30

The number of TCP keep-alive probes (specially formatted TCP frames) to send out before closing the TCP connection.

probe_interval=10-75

The amount of time, in seconds, to wait between sending TCP keep-alive probes.

[*advanced ip options*]

reuse_old_ip={on|off}

When enabled, the device uses an IP address, gateway address, and submask received from DHCP server previously if DHCP is not available. The default is “off.”

autoip={on|off}

When enabled, the device attempts to use the Auto-IP protocol to find an IP address, gateway address, and submask. The default is “on.”

sbr={on|off}

Enables or disables Source Based Routing (SBR). When enabled, each network interface uses a different router. The default is “off.”

Examples

Manually set the device IP v4 address of Ethernet interface 1

```
#> set network index=1 mode_v4=static ip_v4=10.0.0.2
gateway_v4=10.0.0.1 submask_v4=255.255.255.0
```

Use DHCP to find an IPv4 address, gateway address, and submask of Ethernet interface 2

```
#> set network index=2 mode_v4=dhcp
```

See also

- "revert"
- "set autoconnect"
- "set dhcpserver"
- "set service"
- "set wlan"
- "show"

set nfs

Purpose

Configures the Network File System (NFS) settings and displays the status of the NFS service. Network File System (NFS) is a network file system protocol that allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed.

Required permissions

Permissions must be set to one of the following:

• For a user to display the NFS settings: “set permissions s-service=read”

• For a user to display and set the NFS settings: “set permissions s-service=rw”

Syntax

Configure NFS settings

```
set nfs [state={off|on}]
  [server={hostname|ip address}]
  [path=pathname]
  [timeout=5-3600]
  [interval=5-3600]
  [alert_state={off|on}]
  [alert_description=string]
  [alert_priority={normal|high}]
  [alert_type={none|email|snmptrap|all}]
  [alert_subject=string]
  [alert_to=email address]
  [alert_cc=email address]
```

Display current settings

```
set nfs
```

Options

state ={off|on}

Specifies whether the NFS service will be enabled

on

Enable the NFS service.

off

Disable the NFS service.

Default is off.

server ={*host name*|*ip address*}

Specifies the host name or the IP address of NFS server

path=*pathname*

Specifies the full path of directory on NFS server.

timeout=5-3600

Specifies a time out value for waiting response from NFS server.

interval=5-3600

Specifies an interval to check the status of NFS server.

alert_state={off|on}

Specifies whether the alert for changing of the status of NFS service will be enabled.

on

Enable the alert.

off

Disable the alert.

Default is off.

alert_description=*string*

Specifies the description for the alert.

alert_priority={normal|high}

The priority of the alert when the alert type is email.

normal

The alert is sent with normal priority.

high

The alert is sent with high priority.

The default is “normal.”

alert_type={email|snmptrap|all}

Used to determine what kind of an alarm is sent: an e-mail alarm, an SNMP trap or both.

For SNMP traps to be sent, the IP address of the system to which traps are sent must be configured, by issuing a “set snmp” command with the “trapdestip” option. See "set snmp".

email

An email alarm is sent.

snmptrap

An SNMP trap is sent. If snmptrap is specified, the “subject” text is sent with the alarm.

all

Both an email alarm and SNMP trap are sent.

The default is “email.”

alert_subject=*string*

If “alert_type=email,” this option specifies the text to be included in the “subject” field of an alarm-triggered email. If “alert_type=snmptrap,” this option specifies the text to be included in the “NFS Alarm Subject” field of an alarm- triggered SNMP trap.

alert_to=*email address*

The text to be included in the “to” field of an alarm-triggered email.

alert_cc=*email address*

The text to be included in the “cc” field of an alarm-triggered email.

Examples

Enable NFS service

```
#>set nfs state=on server=192.168.100.100 path=/nfsroot
timeout=5 interval=10
```

Display current NFS settings

```
#>set nfs
```

See also

- "show nfs"
- "set smtp"
- "set snmp"

set permissions

Purpose

Used to set user permissions associated with various services and command-line interface (CLI) commands, or display current permission settings.

Commands without permissions

There are no permissions associated with the following commands:

- close
- exit
- help
- info
- quit

Permissions for the "revert" command

For the "revert" command, the permissions associated with the various "set" commands are used, except for the "revert all" command variant, which uses a different mechanism that bypasses the individual "set" commands.

Required permissions

For products with two or more users, permissions must be set to "set permissions s-permissions=read" to display permissions, and "set permissions s-permissions=rw" to display and change permissions. When permissions are set to "set permissions s-permissions=rw," a user cannot set another user's permission level higher than their own level, nor can they raise their own permission level.

Syntax **Set permissions**

```
set permissions [type={user|group}]
  {id=range|name=string}
  [backup={none|execute}]
  [boot={none|execute}]
  [buffers={none|r-self|read|rw-self|
     w-self-r|rw}]
  [connect={none|execute}]
  [display={none|execute}]
  [filesys=(none|read|rw)]
  [kill={none|execute}]
  [newpass={none|rw-self|rw}]
  [ping={none|execute}]
  [python={none|execute}]
  [reconnect={none|execute}]
  [revert-all={none|execute}]
  [rlogin={none|execute}]
  [status={none|execute}]
  [telnet={none|execute}]
  [who={none|execute}]
  [webui={none|execute}
  [s-alarm={none|read|rw}]
  [s-autoconnect={none|r-self|read|rw-self|
     w-self-r|rw}]
  [s-ethernet={none|read|rw}]
  [s-group={none|read|rw}]
  [s-host={none|read|rw}]
  [s-internalmodem={none|read|rw}]
  [s-lcd={none|read|rw}]
  [s-modem={none|read|rw}]
  [s-network={none|read|rw}]
  [s-permissions={none|read|rw}]
  [s-pmodem={none|r-self|read|rw-self|
     w-self-r|rw}]
  [s-portauth={none|read|rw}]
  [s-ppp={none|read|rw}]
  [s-profile={none|r-self|read|rw-self|
     w-self-r|rw}]
  [s-python={none|read|rw}]
  [s-rtstoggle={none|r-self|read|rw-self|
     w-self-r|rw}]
  [s-sdmemory={none|read|rw}]
  [s-serial={none|r-self|read|rw-self|
     w-self-r|rw}]
  [s-service={none|read|rw}]
  [s-snmp={none|read|rw}]
  [s-socket_tunnel={none|read|rw}]
```

```
[s-sysauth={none|read|rw}]
[s-system={none|read|rw}]
[s-tcpserial={none|r-self|read|rw-self|
   w-self-r|rw}]
[s-trace={none|read|rw}]
[s-udpserial={none|r-self|read|rw-self|
   w-self-r|rw}]
[s-usb={none|read|rw}]
[s-user={none|read|rw}]
[s-webui={none|read|rw}]
[s-xbee={none|read|rw}]
```

Display current network configuration options

```
set permissions
```

Options

Permission descriptions

Here are the user permissions and their effects on commands.

none

The command cannot be executed.

execute

The command can be executed.

r-self

The user can execute the "display" portions for both commands if the user is logged in on the specified line.

read

The user can execute the "display" and "set" portions for both commands if the user is logged in on the specified line.

w-self-r

The user can execute the "display" portions for both commands for any line and the "set" portions for both commands if the user is logged in on the specified line.

rw

The user can execute the "display" and "set" portions for both commands for any line.

type={user|group}

Specifies whether the command applies to users or groups. This option defaults to “user.”

id=*range*

Specifies the ID or the range of IDs of the users or groups to be acted on. If omitted, the “name” option must be specified.

name=*string*

Specifies the name of the user or group to be acted on. If omitted, the “id” option must be specified.

backup={none|execute}

Permissions for the “backup” command. (See "backup".)

boot={none|execute}

Permissions for the “boot” command. (See "boot".)

buffers={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “display buffers” and “set buffer” commands. (See "display buffers" and "set buffer")

connect={none|execute}

Permissions for the “connect” command. (See "connect")

display={none|execute}

Permissions for the “display” command. (See "display")

filesys={none|read|rw}

Permissions for user access to the product’s file system.

none

The user cannot access the file system.

read

The user can read the file system.

rw

The user can read and write the file system.

kill={none|execute}

Permissions for the “kill” command. (See "kill")

newpass={none|rw-self|rw}

Permissions for the “newpass” command. (See "newpass")

none

The command cannot be executed.

rw-self

The user can set their own password.

rw

The user can set any user’s password.

ping={none|execute}

Permissions for the “ping” command. (See "ping")

python={none|execute}

Permissions for the “python” command. (See "python")

reconnect={none|execute}

Permissions for the “reconnect” command. (See "reconnect")

revert-all={none|execute}

Permissions for the “revert all” command. (See "revert".) Individual “revert” commands are governed by the permissions for that particular command, but “revert all” uses a different mechanism that bypasses the individual commands.

rlogin={none|execute}

Permissions for the “rlogin” command. (See "rlogin")

status={none|read|rw}

Permissions for the “status” command. (See "status")

telnet={none|execute}

Permissions for the “telnet,” “mode,” and “send” commands. (See "telnet")

webui={none|execute}

Permissions for access to the Web user interface for the device.

none

The user cannot use the Web user interface.

execute

The user can access the Web user interface.

who={none|execute}

Permissions for the “who” command. (See "who")

s-alarm={none|read|rw}

Permissions for the “set alarm” command. (See "set alarm")

s-autoconnect={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set autoconnect” command. (See "set autoconnect")

s-group={none|read|rw}

Permissions for the “set group” command. (See "set group")

s-host={none|read|rw}

Permissions for the “set host” command. (See "set host")

s-internalmodem={none|read|rw}

Permissions for the “set internalmodem” command. (See "set internalmodem")

s-lcd ={none|read|rw}

Permissions for the “set lcd” command. (See "set lcd")

s-modem ={none|read|rw}

Permissions for the “set modem” command. (See "set modem")

s-network={none|read|rw}

Permissions for the “set network” command. (See "set network")

s-permissions={none|read|rw}

Permissions for the “set permissions” command itself.

s-pmodem={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set pmodem” command. (See "set pmodem")

s-portauth ={none|read|rw}

Permissions for the “set portauth” command. (See "set portauth")

s-ppp={none|read|rw}

Permissions for the “set ppp” command. (See "set ppp")

s-profile={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set profile” command. (See "set profile")

s-python={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set python” command. (See "set python")

s-rtstoggle={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set rtstoggle” command. (See "set rtstoggle")

s-sdmemory ={none|read|rw}

Permissions for the “set sdmemory” command. (See "set sdmemory")

s-serial={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set serial” and "set switches" commands. (See "set serial" and "set switches")

s-service={none|read|rw}

Permissions for the “set service” command. (See "set service")

s-snmp={none|read|rw}

Permissions for the “set snmp” command. (See "set snmp")

s-socket-tunnel={none|read|rw}

Permissions for the "set socket_tunnel" command. (See "set socket_tunnel")

s-sysauth ={none|read|rw}

Permissions for the “set sysauth” command. (See "set sysauth")

s-system={none|read|rw}

Permissions for the “set system” command. (See "set system")

s-tcpserial={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set tcpserial” command. (See "set tcpserial")

s-trace={none|read|rw}

Permissions for the “set trace” command. (See "set trace")

s-udpserial={none|r-self|read|rw-self|w-self-r|rw}

Permissions for the “set udpserial” command. (See "set udpserial")

s-usb ={none|read|rw}

Permissions for the “set usb” command. (See "set usb")

s-user={none|read|rw}

Permissions for the “set user” command. (See "set user")

s-xbee={none|read|rw}

Permissions for the “set xbee” command.

s-webui ={none|read|rw}

Permissions for the “set web” command. (See "set web")

Examples

Set group permissions

```
#> set permissions type=group name=gurus newpass=rw-self
s-user=read
```

Set user permissions

```
#> set permissions id=1 newpass=rw s-user=rw s-group=rw
```

See also

- "set user"
- "set group"
- "show"
- “User permissions in ConnectPort LTS products” on page 14

set pmodem

Purpose

Configures various options for modem emulation over TCP/IP, and display current modem-emulation settings.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the modem emulation settings for the line on which they are logged in: “set permissions s-pmodem=r-self”
- For a user to display the modem emulation settings for any line: “set permissions s-pmodem=read”
- For a user to display and set the modem emulation settings for the line on which they are logged in: “set permissions s-pmodem=rw-self”
- For a user to display the modem emulation settings for any line, and set modem emulation settings for the line on which the user is logged in: “set permissions s-pmodem=w-self-r”
- For a user to display and set the modem emulation settings on any line: “set permissions s-pmodem=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Configure modem emulation

The connection-type option, "telnet," applies to both incoming and outgoing calls via the pmodem feature.

```
set pmodem port=range
  [state={on|off}]
  [telnet={on|off}]
```

Display modem-emulation settings

```
set pmodem [port=range]
```

Options

port=*range*

Used to specify the serial port.

state={on|off}

Used to enable or disable modem emulation on a given serial port.

on

Enables modem emulation.

off

Disables modem emulation.

The default is “off”.

telnet

Enables or disables Telnet processing on incoming and outgoing modem-emulation connections.

on

Enables Telnet processing.

off

Disables Telnet processing.

The default is “off”.

Example

```
#> set pmodem port=1 state=on
```

See also

- "revert"
- "show"

set portauth

Purpose

Configures or displays authentication settings of each serial port. Authentication options include None, Local. Radius, and LDAP.

Required permissions

Permissions must be set to one of the following:

- For a user to display the authentication settings for serial ports: “set permissions s-portauth=read”
- For a user to display and set the authentication settings for serial ports: “set permissions s-portauth=rw”

Syntax

Configure port authentication settings

```
set portauth port={port|xbee|internalmodem}
  [authmethod={none|local|radius_server|
  radius_local|local_radius|radius_down_local|
  ldap_server|ldap_local|local_ldap|
  ldap_down_local|]
  [accountingsocket=0-65535]
  [authsocket=0-65535]
  [primary_authsvr ={hostname|ip address}]
  [secondary_authsvr ={hostname|ip address}]
  [primary_acctsvr={hostname|ip address}]
  [secondary_acctsvr ={hostname|ip address}]
  [secret=password]
  [timeout=0-300]
  [retries=1-50]
  [searchbase=string]
  [domainname={hostname|ip address}]
  [ldapsecopt={off|start_tls}]
  [ppp_user=string]
```

Display current port authentication settings for all available serial ports

```
set portauth
```

Display current port authentication settings for a particular serial port

```
set portauth port=port
```

Options

port=(port|xbee|internalmodem)

The serial port number or range of serial ports associated with the port authentication settings. Required when configuring port authentication settings. To configure authentication settings for an XBee port or internal modem, specify port=xbee or port=internalmodem.

authmethod={none|local|radius_server|radius_local|
local_radius|radius_down_local|ldap_server|ldap_local|local_ldap}

The port authentication method to be used for the serial port. Required when configuring port authentication settings. The value of "authmethod" can be one of the following:

none

When selected, user can access the serial port without authentication. This is the factory default setting.

local

When selected, user who registered the local database of ConnectPort LTS through user configuration can only access the serial port.

radius_server

When selected, user who registered the database of Radius server specified can only access the serial port.

radius_local

When selected, the user authentication performed through the Radius server first. If succeeded, user can access the serial port. If failed, user authentication performed through local database of ConnectPort LTS again.

local_radius

When selected, the user authentication performed through the local database of ConnectPort LTS first. If succeeded, user can access the serial port. If failed, user authentication performed through the Radius server again.

radius_down_local

When selected, the user authentication performed through the Radius server first. If succeeded, user can access the serial port. But if the Radius server does not respond to the authentication request from the ConnectPort LTS, user authentication performed through local database of ConnectPort LTS again. But if the authentication through the Radius server is failed, authentication through local database of ConnectPort LTS is not performed and the user cannot access the serial port.

ldap_server

When selected, user who registered the database of LDAP server specified can only access the serial port.

ldap_local

When selected, the user authentication performed through the LDAP server first. If succeeded, user can access the serial port. If failed, user authentication performed through local database of ConnectPort LTS again.

local_ldap

When selected, the user authentication performed through the local database of ConnectPort LTS first. If succeeded, user can access the serial port. If failed, user authentication performed through the LDAP server again.

ldap_down_local

When selected, the user authentication performed through the LDAP server first. If succeeded, user can access the serial port. But if the LDAP server does not respond to the authentication request from the ConnectPort LTS, user authentication performed through local database of ConnectPort LTS again. But if the authentication through the LDAP server is failed, authentication through local database of ConnectPort LTS is not performed and the user cannot access the serial port.

accountingsocket=0-65535

The TCP port to be used for authentication communication. The default port number for Radius authentication is 1813. The primary and the secondary servers are required to use the same TCP port. LDAP authentication method does not support accounting server and socket options.

authsocket=0-65535

The TCP port to be used for authentication communication. The default port number for Radius authentication is 1812 and for LDAP authentication is 389. The primary and the secondary servers are required to use the same TCP port.

primary_authsvr={*hostname*|*ip address*}

The IP address or DNS name of authentication server. This option is compulsory to use the remote authentication method. If this server is down or busy, the authentication query is sent to the secondary server, if specified.

secondary_authsvr={*hostname*|*ip address*}

The IP address or DNS name of secondary authentication server. This option is complementary.

primary_acctsvr={*hostname*|*ip address*}

The IP address or DNS name of accounting server. This option can be specified only when user accounting is required. If this server is down or busy, the accounting information is sent to the secondary server (if it is specified). . LDAP authentication method does not support accounting server and socket options.

secondary_acctsvr={*hostname*|*ip address*}

The IP address or DNS name of secondary accounting server. This option is complementary.

secret =*password*

A kind of password used for encryption of messages between the Radius authentication server and the ConnectPort LTS. The server and device server must use the same secret. The primary and the secondary servers are required to use the same secret.

timeout =0-300

The timeout (specified in seconds) controls how long the ConnectPort LTS will wait for the response from Radius authentication server. Factory default value is 10.

retries =1-50

The retries controls how many time the ConnectPort LTS will try to communicate with the Radius authentication server. Factory default value is 3.

searchbase =*string*

LDAP search base (the distinguished name of the search base object) defines the location in the directory from which the LDAP search begins.

domainname ={*hostname*|*ip address*}

If the LDAP database resides on a Microsoft system, the Domain name for the active directory must be configured on this option. If using a non-Microsoft system, do not use this setting, as it changes the LDAP to comply with Microsoft syntax.

ldapsecopt ={off|start_tls}

Security option for LDAP authentication. If “start_tls” is selected, the StartTLS extended operation is used to secure the communication between ConnectPort LTS and the LDAP Server.

ppp_user=*string*

For inbound PPP connections, this option is the inbound PPP user.

Example

```
#> set portauth port=1 authmethod=radius
primary_authsvr=192.1681.1 secret=teststring
```

See also

- "revert"
- "show "

set portgroup

Purpose

Configures or displays port group settings. Port group is a convenience feature which can be created to send data to multiple ports. Instead of sending data to individual serial ports, data can be sent to all ports in a group simultaneously through a port in a group.

Required permissions

Permissions must be set to one of the following:

- For a user to display the port group
- settings for serial ports: “set permissions s-serial=read”
- For a user to display and set the authentication settings for serial ports: “set permissions s-serial=rw”

Syntax

Add and configure a new port group

```
set portgroup add index=1-16
  [newname=new group name]
  [ports=0-32]
  [showdata={on|off}]
  [sendbyte=1-4096]
  [sendidle=1-65535]
```

Remove port groups

```
set portgroup remove index=1-16
```

Display current port group settings for all available port groups

```
set portgroup
```

Display current port group settings for a particular port group

```
set portgroup name=group name
```

Options

add

Add a port group. A maximum of 16 port groups can be defined.

remove

Remove port groups

index=1-16

Specifies the index number of port group or range of port group indexes to be acted on.

name=*group name*

Specifies the name of port group to be acted on.

ports=0-32

Serial port or range of serial ports. If “port=0” is specified, all ports specified to this port group will be reset.

showdata={on|off}

When enabled, user can see the data from other ports in the same group from a terminal connected to the one of serial ports in the group.

on

Enable showing data from other ports in the same group.

off

Disable showing data from other ports in the same group.

Default is off.

sendbyte=1-4096

Sends data to the other ports in the same group after the specified number of bytes has been received on the serial port. This can be 1 to 4096 bytes. Default is 1024 bytes.

sendidle=1-65535

Sends data to the other ports in the same group after the specified idle time has been passed with no additional data received on the serial port. Range is 1 to 65,535 milliseconds. Default is 1000 milliseconds.

newname =*new group name*

Name of port group when new port group is created.

Example

```
#> set portgroup add index=1 ports=1,2,4-5
newname=testgroup
```

See also

• "show "

set ppp

Purpose

Configures Point-to-Point Protocol (PPP) connections, or displays current PPP settings.

Required permissions

Permissions must be set to one of the following:

- For a user to display the PPP settings: “set permissions s-ppp=read”
- For a user to display and set the PPP settings: “set permissions s-ppp=rw”

Syntax

Add a new ppp setting

```
set ppp add index=1-64
  newname=new username
  connection_type={incoming|outgoing}
```

Remove a PPP setting

```
set ppp remove index=1-64
```

Configure ppp settings

```
set ppp [index=1-64]
  [connection_type={none|incoming|outgoing}]
  [user=username]
  [password=password]
  [pppauth={none|chap|pap|both}]
  [ipaddrmode={ippool|negotiated|static}]
  [ipaddr=ip address]
  [phonenumber1=phone number]
  [phonenumber2=phone number]
  [localipaddr_mode={none|unnumbered|static}]
  [localipaddr=ip address]
  [idletimeout=0-65535]
  [proxy_arp={off|on}]
```

Display ppp current settings

```
set ppp
```

Options

add

Add a PPP setting.

remove

Remove a PPP setting.

index=1-64

PPP user index.

connection_type={none|incoming|outgoing}

The connection type.

none

Disable PPP settings for the user.

incoming

Used for inbound PPP connections. The ConnectPort LTS product will receive connections from other hosts for this user.

outgoing

Used for outbound PPP connection. The ConnectPort LTS product will dial-out to establish PPP connections with external hosts using this user information.

newname=*new username*

User name for new PPP user added

user=*username*

User name for incoming or outgoing PPP connection.

password=*password*

Password for user.

pppauth={none|chap|pap|both}

Determines whether authentication is required for PPP connection and, if so, what kind.

none

The remote user does not require PPP authentication

chap

Challenge Handshake Authentication Protocol (CHAP) authentication is required.

pap

Password Authentication Protocol(PAP) authentication is required.

both

Both CHAP and PAP authentication are required.

The default is “none”

ipaddrmode={ippool|negotiated|static}

The mode of IP address for the peer in an incoming PPP connection.

ippool

The IP address of remote peer will be assigned from the ippool automatically.

negotiated

Allow remote peer to specify remote IP address.

static

The specified IP address for remote peer will be used.

ipaddr=*ip address*

The IP address of remote peer to be used if the ipaddrmode=static

phonenumber1=*phone number*

The primary phone number to dial to request PPP connection.

phonenumber2= *phone number*

The secondary phone number to dial to request PPP connection. If the line of primary phone number is busy, secondary phone number will be used automatically.

localipaddr_mode={none|unnumbered|static}

The mode of IP address for local end in outgoing PPP connection.

none

No the mode of IP address is specified. Outgoing PPP connection is disabled.

unnumbered

Automatically obtain the IP address from remote peer.

static

Request specific IP address.

localipaddr=*ip address*

Specifies the IP address for local end to be requested if the "localipaddrmode=static."

idletimeout=0-65535

The time, in seconds, after which if no data has been transmitted/received over the link, the PPP connection is disconnected.

proxy_arp={off|on}

Whether the proxy ARP entry will be set in the PPP server's ARP table so that ARP Requests can be processed.

on

Enable the proxy ARP entry

off

Disable the proxy ARP entry.

Examples

Set incoming PPP settings

```
#> set ppp add index=2 newname=ibuser
connection_type=incoming
```

Set outgoing PPP settings

```
#> set ppp add index=3 newname=obuser
connection_type=outgoing
```

Remove a PPP setting

```
#>set pppremove index=2
```

Display current PPP settings

```
#>set ppp index=1
```

Change PPP authentication protocol

```
#>set ppp index=3 pppauth=pap
```

See also

"show ppp"

set profile

Purpose

Associates a particular port with one of several port configuration profiles, or displays the current port-profile settings.

Port profiles are a defined set of port configuration settings for a particular use. A port profile reconfigures serial-port settings to the necessary default values in order for the profile to operate correctly.
Port-profile configuration is most often performed through the Web user interface for a device. It is not often specified from the command line, but is available if needed.

ConnectPort LTS devices support several port profiles. Following is the complete set of port profiles. The profiles supported on your product may vary.

- **Console Management profile**: Allows you to access a device's console port over a network connection.
- **Modem Emulation profile**: Allows you to configure the serial port to act as a modem.
- **RealPort profile**: Allows you to map a COM or TTY port to the serial port.
- **TCP Sockets profile**: Allows a serial device to communicate over a TCP network.
- **Tunneling profile**, also known as the **Serial Bridge profile**: Configures one side of a serial bridge. A bridge connects two serial devices over the network, as if they were connected with a serial cable.
- **UDP Sockets profile**: Allows a serial device to communicate using UDP.
- **Custom profile**: An advanced option to allow full configuration of the serial port. This profile allows you to view all settings associated with the serial port.
- **Local Configuration profile:** The Local Configuration profile allows access to the command-line interface when connecting from a serial terminal.

- **Printer profile**: This profile allows you to connect a printer to the serial port
- **Modem profile**: This profile allows you to connect a modem to the serial port in order to establish or receive connections from other systems and modems

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the profile settings for the line on which they are logged in: “set permissions s-profile=r-self”
- For a user to display the profile settings for any line: “set permissions s-profile=read”
- For a user to display and set the profile settings for the line on which they are logged in: “set permissions s-profile=rw-self”
- For a user to display the profile settings for any line, and set modem emulation settings for the line on which the user is logged in: “set permissions s-profile=w-self-r”
- For a user to display and set the profile settings on any line: “set permissions s-profile=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Configure port profile settings

```
set profile port=port
  profile=profile name
  [portsharing={on|off}]
```

Display current port profile settings for all available serial ports

```
set profile
```

Display current port profile settings for a particular serial port

```
set profile port=port
```

Options

port=*port*

The serial port number or range of serial ports associated with the port profile. Required when configuring port profiles.

profile=*profile name*

The port profile to use for the serial port. Required when configuring port profiles. Choosing a particular port profile causes the serial port's configuration to be reset to defaults, and then for the default settings for that port profile to take effect.

Depending on the port-profile choices available for the device, the value of "profile" can be one of the following:

console_management

Associates the Console Management port profile with the port.

modem_emulation

Associates the Modem Emulation port profile with the port.

realport

Associates the RealPort port profile with the port.

tcp_sockets

Associates the TCP Sockets port profile with the port.

tunneling

Associates the Serial Bridge port profile with the port.

udp_sockets

Associates the UDP Sockets port profile with the port.

custom

Associates the Custom port profile with the port.

printer

Associates the Printer port profile with the port.

modem

Associates the Modem port profile with the port.

local_config

Associates the Local Configuration port profile with the port.

portsharing={on|off}

The portsharing option is used to make a serial port be shared between multiple application software. If set to on, a serial port can be accessed by multiple client programs.(up to 4 clients per port).

Note: Port sharing is not supported for RealPort.

Example

```
#> set profile port=1 profile=realport
```

See also

- "revert"
- "show "

set python

Purpose Configures Python programs to execute when the ConnectPort LTS product boots.

Syntax

```
set python [range=1-4]
  [state={on|off}]
  [command=filename]
```

Options

range=1 – 4

The index or indices to view or modify with the command.

state={on|off}

When the state is set to on, the command specified will be run when the device boots.

command=*filename*

The program filename to execute, including any arguments to pass with the program, similar to the arguments for the "python" command. While this option allows for programs to be run from a TFTP server, this use is not recommended. If there are spaces to provide arguments, make sure to wrap the entire command in quotation marks.

Example

```
#> py dia.py
```

See also

- "python"
- *The Digi Python Programming Guide*

set realport

Purpose Configures and displays RealPort-related settings.

Required permissions For products with root and non-root (normal) users, the root user can configure RealPort settings. The normal user can display RealPort settings.

Syntax

Configure RealPort settings

```
set realport [keepalive={on|off}]
  [exclusive={on|off}]
```

Display current RealPort settings

```
set realport
```

Options

keepalive={on|off}

Enables or disables sending of RealPort keepalives. RealPort keepalives are messages inside the RealPort protocol, sent approximately every 10 seconds, to tell whoever is connected that the connection is still alive. RealPort keepalives are different from TCP keepalives, which are done at the TCP layer, and configurable. The default is “on.” As RealPort keepalives generate additional traffic--several bytes every 10 seconds--this option allows you to turn them off. RealPort keepalives may cause issues in environments that are metered for traffic, or that do not require this type of mechanism. In situations such as cellular/mobile wireless communications, when you are paying by the byte, such additional traffic is undesirable when a TCP keepalive can do the same job, and only when the connection is idle. If you want to have the RealPort keepalive set to “off;” consider using a TCP keepalive instead. This is because if the link is not closed properly, you could end up with your port being “locked up” with a dead TCP session, which is why RealPort keepalives were implemented in the first place.

exclusive={on|off}

Enables or disables exclusive mode for RealPort connections. Exclusive mode allows the device to close an existing RealPort connection and establish a new one immediately upon a new connection request from the same IP address. This mode is useful when using RealPort over wide area networks, which can be unstable and where you are charged by the byte (such as cellular or satellite), and you do not wish to incur costs for keep-alive traffic. Exclusive mode allows your application to retain continuity when temporary, unexpected interruptions in network connectivity occur.

Example

```
#> set realport keepalive=on
```

See also

• "set network". The “set network” keepalive options (“idle,” “probe_count,” “probe_interval”) should be configured for various services that are configured by “set service keepalive={on|off},” or clients such as autoconnect (“set autoconnect keepalive={on|off}”).

• "set service"

• "set autoconnect"

set rtstoggle

Purpose

RTS toggle is used to raise RTS when sending data. This command enables or disables RTS toggle on a given serial port, and displays current RTS toggle settings.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the RTS toggle settings for the line on which they are logged in: “set permissions s-rtstoggle=r-self”
- For a user to display the RTS toggle settings for any line:
- “set permissions s-rtstoggle=read”
- For a user to display and set the RTS toggle settings for the line on which they are logged in: “set permissions s-rtstoggle=rw-self”
- For a user to display the RTS toggle settings for any line, and set RCI serial settings for the line on which the user is logged in:
- “set permissions s-rtstoggle=w-self-r”
- For a user to display and set the RTS toggle settings on any line:
- “set permissions s-rtstoggle=rw”
- For a user to display and set the RTS toggle settings on any line:

See "set permissions" for details on setting user permissions for commands.

Syntax

Enable or disable RTS toggle

```
set rtstoggle port=range
  [state={on|off}]
  [predelay= delay]
  [postdelay=delay]
```

Display current RTS toggle settings

```
set rtstoggle [port=range]
```

Options

port=*range*

Used to specify the serial port. Optional on a single-port device.

state={on|off}

Used to enable or disable the RTS toggle feature.

on

Enables the RTS toggle feature.

off

Disables the RTS toggle feature.

The default is “off”.

predelay=*delay*

Specifies the time in milliseconds to wait after the RTS signal is turned on before sending data. The range is 0 to 5000 milliseconds. The default is 0.

postdelay=*delay*

Specifies the time in milliseconds to wait after sending data before turning off the RTS signal. The range is 0 to 5000 milliseconds. The default is 0.

Example

```
#> set rtstoggle state=on predelay=10
```

See also

- "revert"
- "show"

set samba

Purpose Configures and displays Samba service settings.

Required permissions Permissions must be set to one of the following:

- For a user to display the Samba settings: “set permissions s-service=read”
- For a user to display and set the Samba settings:
  “set permissions s-service=rw”

Syntax

Configure Samba settings

```
set samba [state={off|on}]
  [server={hostname|ip address}]
  [path=path]
  [timeout=5-3600]
  [interval=5-3600]
  [user=username]
  [password=password]
  [alert_state={off|on}]
  [alert_description=string]
  [alert_priority={normal|high}]
  [alert_type={email|snmptrap|all}]
  [alert_subject=string]
  [alert_to=email address]
  [alert_cc=email address]
```

Display current settings

```
set samba
```

Options

state={off|on}

Specifies whether the Samba service will be enabled

on

Enable the Samba service.

off

Disable the Samba service.

Default is off.

server={*hostname*|*ip address*}

Specifies the host name or the IP address of Samba server

path=*path*

Specifies the full path of directory on Samba server.

timeout=5-3600

Specifies a time out value for waiting response from Samba server.

interval=5-3600

Specifies an interval to check the status of Samba server.

user=user name

Specifies the name of user for Samba service.

password=*password*

Specifies the password for the user of Samba service.

alert_state={off|on}

Specifies whether the alert for changing of the status of Samba service will be enabled

on

Enable the alert.

off

Disable the alert.

Default is off.

alert_description=*string*

Specifies the description for the alert.

alert_priority={normal|high}

The priority of the alert when the alert type is email.

normal

The alert is sent with normal priority.

high

The alert is sent with high priority.

The default is “normal.”

alert_type={email|snmptrap|all}

Used to determine what kind of an alarm is sent: an e-mail alarm, an SNMP trap or both.

For SNMP traps to be sent, the IP address of the system to which traps are sent must be configured, by issuing a “set snmp” command with the “trapdestip” option. See "set snmp".

email

An email alarm is sent.

snmptrap

An SNMP trap is sent. If snmptrap is specified, the “subject” text is sent with the alarm.

all

Both an email alarm and SNMP trap are sent.

The default is “email.”

alert_subject=*string*

If “alert_type=email,” this option specifies the text to be included in the “subject” field of an alarm-triggered email. If “alert_type=snmptrap,” this option specifies the text to be included in the “Samba Alarm Subject” field of an alarm- triggered SNMP trap.

alert_to=*email address*

The text to be included in the “to” field of an alarm-triggered email.

alert_cc=*email address*

The text to be included in the “cc” field of an alarm-triggered email.

Examples

Enable Samba service

```
#>set samba state=on server=192.168.100.100
path=/sambaroot timeout=5 interval=10 user=admin
password=admin
```

Display current Samba settings

```
#>set samba
```

See also

- "show samba"
- "set smtp"
- "set snmp"

set sdmemory

Purpose Configures and displays SD memory device settings.

Required permissions Permissions must be set to one of the following:

- For a user to display the SD memory settings:
  "set permissions s-sdmemory=read"
- For a user to display and set the SD memory settings:
  "set permissions s-sdmemory=rw"

Syntax

Enable/Disable SD memory

```
set sdmemory state={on|off}
```

Format SD memory card

```
set sdmemory [state={off|on}]
  [format]
  [fstype={ext2|vfat}]
```

Display SD memory information

```
set sdmemory
```

Options

state={on|off}

Specifies whether the SD memory will be enabled

on

Enable the SD memory.

off

Disable the SD memory.

format

Format the device, using a default file system type of **ext2**. To format with an alternate file system type, use the "fstype" option.

fstype={ext2|vfat}

The file system type.

ext2

ext2 or second extended filesystem.

vfat

Virtual file allocation table filesystem.

Example

Format the SD memory card

```
#>set sdmemory format
```

See also "show sdmemory"

set serial

Purpose

Sets and displays general serial configuration options, such as baud rate, character size, parity, stop bits, and flow control.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the serial settings for the line on which they are logged in: “set permissions s-serial=r-self”
- For a user to display the serial settings for any line: “set permissions s-serial=read”
- For a user to display and set the serial settings for the line on which they are logged in: “set permissions s-serial=rw-self”
- For a user to display the serial settings for any line, and set serial settings for the line on which the user is logged in: “set permissions s-serial=w-self-r”
- For a user to display and set the serial settings on any line: “set permissions s-serial=rw”
- For a user to display and set the RTS toggle settings on any line: “set permissions s-serial=rw”

See "set permissions" for details on setting user permissions for commands. Permissions for "set serial" also apply to the "set switches" command. See "set switches".

Syntax

Set general serial options

```
set serial port={range|internalmodem|xbee}
  [altpin={on|off}]
  [baudrate=bps]
  [databits ={5|6|7|8}]
  [parity={none|even|odd|mark|space}]
  [stopbits ={1|2}]
  [flowcontrol={hardware|software|none|custom}]
  [sigsonopen=(none|rtsdtr)]
  [customflow={none|rtscts|dtrdsr|ixonixoff}]
```

Display current serial options

```
set serial [port=range]
```

Options

port={*range*|internalmodem}xbee}

Used to specify the serial port. Optional on a single-port device. To configure settings for an internal modem port, specify "port=internalmodem" To configure settings for an XBee port, specify "port=xbee."

altpin={on|off}

Determines whether the altpin option, which swaps DCD with DSR so that eight-wire RJ-45 cables can be used with modems, is used:

on

The altpin option is used.

off

The altpin option is not used.

The default is "off".

baudrate=*bps*

The baud rate in bits per second. The default is 9600.

databits ={5|6|7|8}

The character size, which can be 5, 6, 7, or 8 bits. The default is 8.

flowcontrol={none|hardware|software|custom}

Specifies which kind of flow control is used on the line.

none

No flow control.

hardware

Hardware flow control (RTS/CTS).

software

Software flow control (Xon/Xoff).

custom

Custom flow control, as specified by the “customflow” option.

The default is “none.”

parity={none|even|odd|mark|space}

The parity used for the line.

none

No parity.

even

Even parity.

odd

Odd parity.

mark

Mark parity.

space

Space parity.

The default is “none.”

stopbits ={1|2}

The number of stop bits per character to use on this line. The value used here must match the setting on the device connected to this port. Use 1 or 2 stop bits.

The default is 1 stop bit.

sigsonopen ={none|rtsdtr}

Determines the signal behavior of the serial port when ports are opened and closed by client from the remote site. When set to none, the open/close of a port by remote client will not modify the signals state. When set to rtsdtr, the outgoing signals will be raised on open and dropped on close by remote client. The flow control configuration of an outgoing signal takes priority over any behavior specified by the sigsonopen parameter. Please note that only the TCP connection from the remote site will be effective to sigsonopen option of opening/closing of a serial port.

customflow ={none|rtscts|dtrdsr|ixonixoff}

The custom flow control used on the line. This option allows for specifying multiple signals for flow control in non-standard ways, with combinations for the same direction of data transfer; see the example below.

Examples

Set baud rate and flow control

```
#> set serial baudrate=9600 flowcontrol=hardware
```

Set custom flow control

This command sets receive flow control to be RTS and both CTS and DSR to be used for transmit flow control.

```
#> set serial customflow=rts,cts,dsr
```

See also

- "revert"
- "show"

set service

Purpose

Enables and disable network , changes the network port on which a given service listens, and displays the entire service table, or an entry in the service table.

Exercise caution in enabling and disabling network services, particularly disabling them. Changing certain settings can render your product inaccessible. For example, if you disable Advanced Digi Discovery Protocol (ADDP), the device will not be discovered on a network, even if it is actually connected. If you disable HTTP and HTTPS, the Web interface can be disabled. Disabling basic services such as Telnet, Rlogin, etc. can make the Command-Line interface inaccessible.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-service=read” to display network service settings, and “set permissions s-services=rw” to display and change network service settings. See "set permissions" for details on setting user permissions for commands.

Syntax

Enable/disable network services or change network port for service

```
set service [range=range]
  [state={on|off}]
  [ipport=network port]
  [keepalive={on|off}]
  [nodelay={on|off}]
  [delayed_ack=0-1000]
```

Display service table or entries in the table

```
set service [range=range]
```

Options

range=*range*

Used to specify the index of the network service to which the rest of the command's options apply. For more information on using this option, see "Index numbers and changing default port numbers"

state={on|off}

Used to enable or disable a given network service.

ipport=*network port*

Used to change the network port on which a given network service listens. See "Supported network services and their default network port numbers" for more information on the network services available.

keepalive={on|off}

Indicates whether or not TCP keepalives will be sent for specified range of network services. If set to on, keepalives will be sent, if it is off, keepalives will not be sent.

Configurable TCP keepalive parameters, for example, how many keepalives to send and when to send them are configured globally via the "set network" command (see "set network").

nodelay={on|off}

Used to allow unacknowledged or smaller-than-maximum-segment-sized data to be sent for the specified range of network services.

The "nodelay" option disables Nagle's algorithm, which is on by default, for some TCP services. The purpose of Nagle's algorithm is to reduce the number of small packets sent. The algorithm establishes not sending outgoing data when there is either unacknowledged sent data, or there is less-than-maximum segment size (typically around 1500 bytes for Ethernet) worth of data to be sent. While this algorithm allows for efficient data transmission, there are times when it is desirable to disable it.

delayed_ack=0-1000

The time, in milliseconds, to delay sending ACK packets in response to received data for the specified range of network services. The default is 200 milliseconds.

Setting this option to 0 (zero) sends an ACK packet back acknowledge the received data immediately. Setting it to any other value means that the ACK packet will be sent after the specified time. If the network services generate new data during that time, the ACK packet will be sent along with the data packet.

You can use this setting to avoid congestion and reduce network traffic, However, do not change this option from its default setting unless you have a solid understanding of network services and data transmission, or have been instructed to make the change.

Supported network services and their default network port numbers

The following table shows the network services controlled by the "set services" command, the services provided, and the default network port number for each service.

In products that have multiple serial ports, the network port number defaults for various services are set based on the following formula:

base network port number + serial port number

For example, the Telnet Passthrough service is set to network port 2001 for serial port 1, 2002 for serial port 2, 2003 for serial port 3, etc.

If you change a network port for a particular service, that is the only network port number that changes. That change does not carry over to the other network ports. For example, if you change the network port number Telnet Passthrough from 2001 to 3001, that does not mean that the other network ports will change to 3002, 3003, etc.

There are two types of network services available:

• Basic services, which are accessed by connecting to a particular well-known network port.

• Passthrough services, in which a particular serial port is set up for a particular type of service.

To use the service, users must both use the correct protocol and specify the correct network port. The serial port profile must also be set to a profile that allows passthrough, such as the Console Management.

For example, assuming default service ports and using a Linux host, here is how a user would access the Telnet passthrough services:

```
#> telnet digi16 2101
```

Service	Services provided	Default network port number
Advanced Digi Discovery Protocol (ADDP), also known as Device Discovery	Discovery of Digi devices on a network.	2362
Encrypted (Secure) RealPort	Secure Ethernet connections between COM or TTY ports and device servers or terminal servers.	1027
Hypertext Transfer Protocol (HTTP), also known as Web Server	Access to web pages for configuration that can be secured by requiring a user login.	80
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), also known as Secure Web Server	Access to web pages for configuration that can be secured by requiring a user login, with encryption for greater security.	443
Line Printer Daemon (LPD)	Allows network printing over a serial port.	515
RealPort	A virtual connection to serial devices, no matter where they reside on the network.	771
Remote login (Rlogin)	Allows users to log in to the ConnectPort LTS product and access the command-line interface via Rlogin.	513
Remote shell (Rsh)	Allows users to log in to the ConnectPort LTS product and access the command-line interface via Rsh.	514
Secure Shell (SSH)	Allows users secure access to log in to the ConnectPort LTS product and access the command-line interface.	22
Secure Shell (SSH) Passthrough	Accessing a specific serial port set up for SSH.	2501

Service	Services provided	Default network port number
Secure Socket Service	Authentication and encryption for ConnectPort LTS products.	2601
Simple Network Management Protocol (SNMP)	Managing and monitoring the ConnectPort LTS product. If you want to run SNMP, but in a more secure manner, note that SNMP allows for "sets" to be disabled. This securing is done in SNMP itself, not through this command.	161
Transmission Control Protocol (TCP) Echo	Used for testing the ability to send and receive over a TCP connection, similar to a ping.	7
Telnet	Allows users an interactive Telnet session to the ConnectPort LTS product's command-line interface.	23
Telnet Passthrough	Allows a Telnet connection directly to the serial port, often referred to as reverse Telnet.	2001
Transmission Control Protocol (TCP) Passthrough	Allows a raw socket connection directly to the serial port, often referred to as reverse sockets.	2101
User Datagram Protocol (UDP) echo	Used for testing the ability to send and receive over a UDP connection, similar to a ping.	7
User Datagram Protocol (UDP) Passthrough	Allows raw data to be passed between the serial port and UDP datagrams on the network.	2101
Socket Tunnel Server	Allows a Socket Tunnel connection between ConnectPort LTS product and the remote device.	4401

Index numbers and changing default port numbers

An index number is assigned to each of these services. The index numbers assigned can vary over time. If you want to change the network port number for a service, enter a “set service” or “show service” command to display the current index number assigned to all services. Locate the service for which you want to change the network port number, and note the index number for the service. Enter a “set service” command, specify that index number for the “range” option, and the new network port number for the “ipport” option.

For example, to change the network port number for the Telnet basic service from its default port number, 23, you would enter the following “set service” command:

```
#> set service
```

which displays the services defined in and their current network port number assignments:

```
Service configuration
no.   state   port    keepalive   nodelay   dlyd_ack
  1    on     2362    none        none      200   ADDP Service
  2    on     1027    off         none      200   Encrypted RealPort Service
  3    on     515     off         off       200   Line Printer Daemon
  4    on     771     off         none      200   RealPort Service
  5    on     513     off         off       200   Rlogin Service
  6    on     514     off         none      200   Rsh Service
  7    on     161     none        none      200   SNMP Service
  8    on     22      off         off       200    SSH Service
  9    on     23      off         off       200    Telnet Service
 10    on     80      none        none      200   HTTP Service
 11    on     443     none        none      200   HTTPS Service
 12    on     7       off         off       200   TCP Echo Service
 13    on     7       off         off       200   UDP Echo Service
 14    on     50000   none        none      200   Modem Emulation(Pool)
 15    on     2001    off         off       200   Telnet Server(Port 1)
 16    on     2101    off         off       200   TCP Server(Port 1)
 17   off     2101    off         off       200   UDP Server(Port 1)
 18    on     2501    off         off       200   SSH Server(Port 1)
 19    on     2601    off         off       200   Secure Socket Service(Port 1)
 20   off     50001   off         off       200   Modem Emulation(Port 1)
 21   off     none    none        none      none   RealPort Service(Port 1)
 22    on     2002    off         off       200   Telnet Server(Port 2)
```

Note that the index number assigned to the Telnet basic service is 9. You would then specify that index number for the “range” option, and the new network port number for the “ipport” option:

```
#> set service range=9 ipport=100
```

Examples

Disable service

```
#> set service range=1 state=off
```

Change the network port (ipport) of a service

```
#> set service range=1 ipport=500
```

Displaying the service table

In this example, the “set service” command displays the entire service table.

```
#> set service
```

Displaying an entry in the service table

In this example, the “set service” command displays a range of entries in the service table.

```
#> set service range=2-4
```

Allow outgoing data that is unacknowledged or less than maximum segment size.

```
#> set service ra=5 nodelay=on
```

See also

- "revert"
- "set network"
- "set passthrough" for information on network services and applications that are enabled and disabled by default when a ConnectPort LTS product is configured for IP passthrough.
- "show"

set smtp

Purpose

Configures the Simple Mail Transfer Protocol(SMTP) server, or displays current SMTP settings.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-service=read” to display the SMTP service settings, and “set permissions s-service=rw” to display and change the SMTP service settings. See "set permissions" for details on setting user permissions for commands.

Syntax

Configure SMTP settings

```
set smtp [state={off|on}]
  [mode={auth|woauth|pop}]
  [smtp_server={hostname|ip address}]
  [user=username]
  [password=password]
  [from=email address]
```

Display current settings

```
set smtp
```

Options

state={off|on}

Specifies whether the SMTP service will be enabled

on

Enable the SMTP service.

off

Disable the SMTP service.

Default is off.

mode={auth | woauth|pop}

Specifies the authentication method for SMTP AUTH authentication.

auth

Enable the SMTP authentication.

woauth

Disable the SMTP authentication.

pop

Enable the POP before SMTP Authentication.

user=*username*

Specifies the user name for SMTP authentication

password=*password*

Specifies the password of the user for SMTP authentication.

from=*email address*

Specifies the sender’s e-mail address.

Examples

Enable SMTP service

```
#>set smtp state=on mode=auth
smtp_server=192.168.100.100 user=test
password=test1234 from=lts@digi.com
```

Display current SMTP settings

```
#>set smtp
```

See also

- "revert"
- To disable and enable SMTP alarm traps, see "set alarm".

set snmp

Purpose

Configures the Simple Network Management Protocol (SNMP) agent, or displays current SNMP settings.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-snmp=read” to display SNMP service settings, and “set permissions s-snmp=rw” to display and change SNMP service settings. See "set permissions" for details on setting user permissions for commands.

Syntax

Set SNMP settings

```
set snmp[snmpv1v2c options]
  [snmpv3 options]
  [snmp trap options]
  [snmpv3 trap options]
```

Where:

```
[snmpv1v2c options] are:
  [snmpv1v2_enabled={off|on}]
  [publiccommunity=string]
  [privatecommunity= string
  [snmpv1v2_permission={get_only|get_set}]
```

```
[snmpv3 options] are:
  [snmpv3_enabled={off|on}]
  [security_level={auth_nopriv|auth_priv|
  noauth_nopriv}]
  [snmpv3_permission={get_only|get_set}]
  [auth_user=username]
  [auth_protocol={md5|sha}]
  [auth_pwd=password]
  [priv_protocol={des|aes}]
  [priv_pwd=password]
```

[*snmp trap options*] are:
  [trap_version={none|v1|v2c|v3}]
  [trap_community=*string*]
  [trapdestip={*ip address*|*fqdn*}]
  [trapsecdest={*ip address*|*fqdn*}]
  [authfailtrap={off|on}]
  [coldstarttrap={off|on}]
  [linkuptrap={off|on}]
  [logintrap={off|on}]

[*snmpv3 trap options*] are:
  [trap_security_level={auth_nopriv|auth_priv|
  noauth_nopriv}]
  [trap_auth_user=*username*]
  [trap_auth_protocol={md5|sha}]
  [trap_auth_pwd=*password*]
  [trap_priv_protocol={des|aes}]
  [trap_priv_pwd=*password*]
  [trap_engine_id=*string*]

Display SNMP settings

```
set snmp
```

Options **[*snmpv1v2c options*]**

snmpv1v2_enabled={off|on}

Enables or disables the accessing of SNMP-managed objects through SNMP v1/v2c protocol.

off

Disables the accessing of SNMP-managed objects through SNMP v1/v2c protocol.

on

Enables the accessing of SNMP- managed objects through SNMP v1/v2c protocol.

publiccommunity=*string*

The password required to "get" SNMP-managed objects(v1/v2c). The default is "public".

privatecommunity=*string*

The password required to "set" SNMP-managed objects(v1/v2c). The default is "private".

snmpv1v2_permission={get_only|get_set}

Allow SNMP clients to set device settings through SNMP (v1/v2c).

get_only

Disabled the capability for users to issue SNMP "set" commands uses use of SNMP read-only for the ConnectPort LTS product.

get_set

Enabled the capability for users to issue SNMP "set" commands uses use of SNMP read-only for the ConnectPort LTS product.

[*snmpv3 options*]

snmpv3_enabled={off|on}

Enables or disables use of SNMP version 3.

off

Disables the accessing of SNMP-managed objects through SNMP v3 protocol.

on

Enables the accessing of SNMP-managed objects through SNMP v3 protocol.

security_level={auth_nopriv|auth_priv|noauth_nopriv}

Indicates the security level of the user with regard to authentication and privacy

auth_nopriv

Set the security level to use authentication only.

auth_priv

Set the security level to use both authentication and privacy.

noauth_nopriv

Set the security level not to use both authentication and privacy.

snmpv3_permission={get_only|get_set}

Allow SNMP clients to set device settings through SNMP (v3)

get_only

Disabled the capability for users to issue SNMP “set” commands uses use of SNMP read-only for the ConnectPort LTS product.

get_set

Enabled the capability for users to issue SNMP “set” commands uses use of SNMP read-only for the ConnectPort LTS product.

auth_user=*username*

SNMPv3 User name who is authenticated to communicate with the SNMP engine.

auth_protocol={md5|sha}

Specifies the authentication protocol algorithm.

md5

Set MD5 algorithm as authentication protocol.

sha

Set SHA algorithm as authentication protocol.

auth_pwd=*password*

Set the password for authentication.

priv_protocol={des|aes}]

Specifies the privacy protocol algorithm.

des

Set DES algorithm as privacy protocol.

aes

Set AES algorithm as privacy protocol.

priv_pwd=*password*

Set the password for privacy.

[*snmp trap options*]

trap_version={none|v1|v2c|v3}

Specify the version of SNMP protocol to use for SNMP trap configuration.

none

Disable SNMP trap.

v1

Use SNMP v1 protocol for SNMP trap.

v2c

Use SNMP v2c protocol for SNMP trap.

v3

Use SNMP v3 protocol for SNMP trap.

trap_community=*string*

Set community string to be sent with SNMP trap.

trapdestip=*ip address or fqdn*

Used to configure the IP address of the system to which the agent should send traps. To enable any of the traps, a non-zero value for trapdestip must be specified. The ”trapdestip” option is required in order for alarms to be sent in the form of SNMP traps.

trapsecdest=*ip address or fqdn*

Secondary trap destination IP address; an optional configuration.

authfailtrap={off|on}

Enables or disables the sending of authentication failure traps.

on

Enables the sending of authentication failure traps.

off

Disables the sending of authentication failure traps.

The default is “off”.

coldstarttrap ={off|on}

Enables or disables the sending of cold start traps.

on

Enables the sending of cold start traps.

off

Disables the sending of cold start traps.

The default is “off”.

linkuptrap={off|on}

Enables or disables the sending of link up traps.

on

Enables the sending of link up traps.

off

Disables the sending of link up traps.

The default is “off”.

logintrap={off|on}

Enables or disables the sending of login traps.

on

Enables the sending of login traps.

off

Disables the sending of login traps.

The default is “off”.

[*snmpv3 trap options*]

trap_security_level={auth_nopriv|auth_priv|noauth_nopriv}

Indicates the security level of the user with regard to authentication and privacy for SNMP v3 trap.

auth_nopriv

Set the security level to use authentication only.

auth_priv

Set the security level to use both authentication and privacy.

noauth_nopriv

Set the security level not to use both authentication and privacy.

trap_auth_user=*username*

The SNMPv3 trap user name that is authenticated to communicate with the SNMP engine.

trap_auth_protocol={md5|sha}

Specifies the authentication protocol algorithm for SNMP v3 trap.

md5

Set MD5 algorithm as authentication protocol.

sha

Set SHA algorithm as authentication protocol.

trap_auth_pwd=*password*

SNMPv3 trap authentication password.

trap_priv_protocol={des|aes}

SNMPv3 trap privacy protocol.

des

Set DES algorithm as privacy protocol.

aes

Set AES algorithm as privacy protocol.

trap_priv_pwd=*password*

Specifies the SNMPv3 trap privacy password.

trap_engine_id=*string*

Specifies SNMPv3 trap engine ID.

Examples

Enable authentication failure traps

```
#> set snmp trapdestip=10.0.0.1 authfailtrap=on
```

Specify a new private community string

```
#> set snmp privatecommunity=”StLucia72!”
```

See also

- "revert".
- To disable and enable SNMP, use the “set service” command. See "set service."
- To disable and enable SNMP alarm traps, see "set alarm."

set socket_tunnel

Purpose

Configures a socket tunnel. A socket tunnel can be used to connect two network devices: one on the ConnectPort LTS product's local network and the other on the remote network. This is especially useful for providing SSL data protection when the local devices do not support the SSL protocol.

One of the endpoint devices is configured to initiate the socket tunnel. The tunnel is initiated when that device opens a TCP socket to the ConnectPort LTS product on the configured port number. The ConnectPort LTS product then opens a separate connection to the specified destination host. Once the tunnel is established, the ConnectPort LTS product acts as a proxy for the data between the remote network socket and the local network socket, regardless of which end initiated the tunnel.

The socket tunnel feature is most useful for devices with two interfaces. It could also be used as a connection proxy on a single-interface device. One way the socket tunnel feature would be very useful in a single interface device is when the device has the capability to use specified keys, and other devices connected to it do not have that capability. Using the socket tunnel feature, the device with the key capability basically becomes a security gatekeeper for simple devices that cannot use PKI certificates.

Required permissions

For products with two or more users, permissions must be set to "set permissions s-socket-tunnel=read" to display socket tunnel settings, and "set permissions s-socket-tunnel=rw" to display and change socket tunnel settings, settings. See "set permissions" for details on setting user permissions for commands.

Syntax

Configure a socket tunnel

```
set socket_tunnel [state={on|off}]
  [timeout={0|seconds}] {0 is no timeout}
  [from_hostname={name|ip address}
  [from_port=port number]
  [from_protocol={tcp|ssl}]
  [to_hostname={name|ip address}]
  [to_port=port number]
  [to_protocol={tcp|ssl}]
```

Display current socket tunnel settings

```
set socket_tunnel
```

Options

state={on|off}

Enables or disables the configured socket tunnel.

timeout={0|*seconds*}] {0 is no timeout}

The timeout (specified in seconds) controls how long the tunnel will remain connected when there is no tunnel traffic. If the timeout value is zero, then no timeout is in effect and the socket tunnel will stay up until some other event causes it to close.

from_hostname={*name*|*ip address*}

The initiating host: the hostname or IP address of the network device that initiates the socket tunnel.

from_port=*port number*

The initiating port: the port number that the ConnectPort LTS product uses to listen for the initial socket tunnel connection.

from_protocol={tcp|ssl}

The initiating protocol: the protocol used between the device that initiates the socket tunnel and the ConnectPort LTS product. Currently, TCP and SSL are the two supported protocols.

to_hostname={*name*|*ip address*}

The destination host: The hostname or IP address of the destination network device.

to_port=*port number*

The destination port: the port number that the ConnectPort LTS product uses to make a connection to the destination device.

to_protocol={tcp|ssl}

The destination protocol: the protocol used between ConnectPort LTS product and the destination device. Currently, TCP and SSL are the two supported protocols. This protocol does not need to be the same for both connections.

See also

- "revert"
- "show"
- The section on socket tunnel settings in the *ConnectPort LTS User's Guide*.

set switches

Purpose

Configures Multiple Electrical Interface (MEI) settings on a per-port basis, and displays current MEI settings. MEI settings include the type of electrical interface (EIA-232 or EIA-485), the number of differential wires used for communication, and whether termination and biasing resistors are used.

Required permissions

The serial permissions associated with the "set serial" command also apply to this command. For products with two or more users, to use this command, permissions must be set to one of the following.

- For a user to display the serial settings for the line on which they are logged in: “set permissions s-serial=r-self”
- For a user to display the serial settings for any line: “set permissions s-serial=read”
- For a user to display and set the serial settings for the line on which they are logged in: “set permissions s-serial=rw-self”
- For a user to display the serial settings for any line, and set serial settings for the line on which the user is logged in: “set permissions s-serial=w-self-r”
- For a user to display and set the serial settings on any line: “set permissions s-serial=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Configure MEI settings

```
set switches [port=range]
  [mode={232|485}]
  [wires={two|four}]
  [termination={on|off}]
```

Display current MEI settings

```
set switches
```

Options

range=*range*

The port or range of ports to which this command applies.

mode={232|485}

Selects the electrical interface of the serial port. The selected value determines whether the "wires" and "termination" options are meaningful.

232

The serial port uses electrical interface EIA-232. This interface uses independent wires to transmit and receive data, which allows data to be sent and received between devices simultaneously.

485

The serial port uses electrical interface EIA-485. This mode can also be used for EIA-422 connections. This interface uses two wires to both transmit and receive data. This interface also allows for multiple transmitters and receivers to be easily connected together.

The "wires" and "termination" command options specifically apply to serial ports in EIA-485 mode.

The default is "232."

wires={two|four}

Applies when the serial port is running in EIA-485 mode only. Selects the number of differential wires used for communication and implicitly determines the duplex of the connection.

two

The serial port operates in two-wire mode. This mode is a half-duplex connection with shared transmit and receive wires.

four

The serial port operates in four-wire mode. This mode is a full-duplex connection with independent transmit and receive pairs.

The default is "four."

termination={on|off}

Applies when the serial port is running in EIA-485 mode only. Determines whether termination and biasing resistors are used across the lines.

on

Termination and biasing resistors are enabled across the lines. Termination should be set to "on" if this node is an endpoint of the 485 network. Biasing should be used in at least one unit in a two-wire environment.

off

Termination and biasing resistors are disabled across the lines.

The default is "off."

Examples

Configure standard EIA-232 communication

```
#> set switches port=1 mode=232
```

Configure a half-duplex EIA-485 endpoint

```
#> set switches port=1 mode=485 wires=two
termination=on
```

Configure a full-duplex 422 interior node

```
#> set switches port=1 mode=485 wires=four
termination=off
```

See also

• "display". The “display switches” command displays the current switch settings.

• "revert". The “revert switches” command reverts the “set switches” configuration.

set sysauth

Purpose

Configures or displays authentication settings for the command-line interface or web server. The following authentication options are provided:

- Local
- Radius
- LDAP

Required permissions

Permissions must be set to one of the following:

- For a user to display the authentication settings for CLI or Web server: "set permissions s-sysauth=read"
- For a user to display and set the authentication settings for CLI or Web server: "set permissions s-sysauth=rw"

Syntax

Configure authentication settings of CLI or Web server

```
set sysauth index=(1-2)
  authmethod={local|radius_server|
  radius_local|local_radius|radius_down_local|
  ldap_server|ldap_local|local_ldap|
  ldap_downlocal}
  [accountingsocket=0-65535]
  [authsocket=0-65535]
  [primary_authsvr={hostname|ip address}]
  [secondary_authsvr={hostname|ip address}]
  [primary_acctsvr={hostname|ip address}]
  [secondary_acctsv={hostname|ip address}]
  [secret=password]
  [timeout=0-300]
  [retries=1-50]
  [searchbase=string]
  [domainname={hostname|ip address}]
  [ldapsecopt={off|start_tls}]
```

Display current authentication settings of CLI or Web server

```
set sysauth
```

Options

index=1-2

The index number associated with the system authentication settings. Required when configuring system authentication settings. To configure authentication settings for Web server, specify “index=1.” To configure authentication settings for CLI access, specify “index=2.”

authmethod= {local|radius_server|radius_local| local_radius|radius_down_local|ldap_server|ldap_local|local_ldap| ldap_down_local}

The authentication method to be used for CLI or Web server. Required when configuring system authentication settings.

local

The user who registered the local database of ConnectPort LTS through the user can only access the CLI or Web server.

radius_server

The user who registered the database of Radius server specified can only access the CLI or Web server.

radius_local

User authentication is performed through the Radius server first. If authentication is successful, the user can access the CLI or Web server. If authentication fails, user authentication is performed through local database of ConnectPort LTS again.

local_radius

User authentication is performed through the local database of ConnectPort LTS first. If authentication is successful, the user can access the CLI or Web server. If authentication fails, user authentication is performed through the Radius server again.

radius_down_local

User authentication is performed through the Radius server first. If authentication is successful, the user can access CLI or Web server. If the Radius server does not respond to the authentication request from the ConnectPort LTS, user authentication is performed through local database of ConnectPort LTS again. If authentication through the Radius server fails, authentication through the local database of the ConnectPort LTS is not performed and the user cannot access the CLI or Web server.

ldap_server

Only the user who registered the database of LDAP server specified can access CLI or Web server.

ldap_local

User authentication is performed through the LDAP server first. If authentication is successful, the user can access CLI or Web server. If authentication fails, user authentication is performed through local database of ConnectPort LTS again.

local_ldap

User authentication is performed through the local database of ConnectPort LTS first. If authentication is successful, the user can access CLI or Web server. If authentication fails, user authentication is performed through the LDAP server again.

ldap_down_local

User authentication performed through the LDAP server first. If succeeded, user can access CLI or Web server. But if the LDAP server does not respond to the authentication request from the ConnectPort LTS, user authentication performed through local database of ConnectPort LTS again. But if the authentication through the LDAP server is failed, authentication through local database of ConnectPort LTS is not performed and the user cannot access CLI or Web server.

accountingsocket=0-65535

The TCP port to be used for authentication communication. The default port number for Radius authentication is 1813. The primary and the secondary servers are required to use the same TCP port. LDAP authentication method does not support accounting server and socket options.

authsocket=0-65535

The TCP port to be used for authentication communication. The default port number for Radius authentication is 1812 and for LDAP authentication is 389. The primary and the secondary servers are required to use the same TCP port.

primary_authsvr={*hostname*|*ip address*}

The IP address or DNS name of authentication server. This option is required for the remote authentication method. If this server is down or busy, the authentication query is sent to the secondary server, if specified.

secondary_authsvr={*hostname*|*ip address*}

The IP address or DNS name of secondary authentication server. This option is optional.

primary_acctsvr={*hostname*|*ip address*}

The IP address or DNS name of accounting server. This option can be specified only when user accounting is required. If this accounting server is down or busy, the accounting information is sent to the secondary server, if specified. . The LDAP authentication method does not support accounting server and socket options.

secondary_acctsvr={*hostname*|*ip address*}

The IP address or DNS name of secondary accounting server. This option is optional.

secret=*password*

A kind of password used for encryption of messages between the Radius authentication server and the ConnectPort LTS. The server and device server must use the same secret. The primary and the secondary servers are required to use the same secret.

timeout=0-300

The timeout (specified in seconds) controls how long the ConnectPort LTS will wait for the response from Radius authentication server. Factory default value is 10.

retries=1-50

Specifies how many times the ConnectPort LTS will try to communicate with the Radius authentication server. Factory default value is 3.

searchbase =*string*

The name of the LDAP search base; that is, the distinguished name of the search base object. This setting defines the location in the directory from which the LDAP search begins.

domainname={*hostname*|*ip address*}

If the LDAP database resides on a Microsoft system, the domain name for the active directory must be configured on this option. If using a non-Microsoft system, do not use this setting, as it changes the LDAP to comply with Microsoft syntax.

ldapsecopt ={off|start_tls}

Security option for LDAP authentication. If start_tls is selected, the StartTLS extended operation is used to secure the communication between ConnectPort LTS and the LDAP Server.

Example

```
#> set sysauth index=1 authmethod=radius
primary_authsvr=192.1681.1 secret=teststring
```

See also

- "revert"
- "show "

set syslog

Purpose Used for managing SYSLOG settings and showing the status of the SYSLOG service. The SYSLOG service sends serial port data to a SYSLOG server.

Required permissions Permissions must be set to one of the following:

- For a user to display the Samba settings: “set permissions s-service=read”
- For a user to display and set the Samba settings: “set permissions s-service=rw”

Syntax

Configure SYSLOG settings

```
set syslog [state={off|on}]
  [server={hostname|ip address}]
  [facility={Local0|Local1|Local2|Local3|Local4|
  Local5|Local6|Local7}]
```

Display current settings

```
set syslog
```

Options

state ={off|on}

Specifies whether the Syslog service will be enabled

on

Enable the Syslog service.

off

Disable the Syslog service.

Default is off.

server={*hostname*|*ip address*}

Specifies the host name or the IP address of Syslog server.

facility=(Local0|Local1|Local2|Local3|Local4|Local5| Local6|Local7)

Specifies the facility level used for logging. Facility levels are used to label information as it is sent to the SYSLOG service. They allow for different types of data to be handled separately at the SYSLOG server.

Examples

Enable Syslog service

```
#>set syslog state=on server=192.168.100.100
facility=Local0
```

Display current Syslog settings

```
#>set syslog
```

See also "show syslog"

set system

Purpose

Configures and displays system-identifying information, such as a description of the device, its location, and a contact person.

Required permissions

For products with two or more users, permissions must be set to “set permissions s-service=read” to display network service settings, and “set permissions s-services=rw” to display and change network service settings.

Syntax

Change system-identifying information

```
set system [description=string]
  [location=string]
  [contact=string]
```

Display system-identifying information

```
set system
```

Options

description=*string*

A description of this device. The maximum length is 64 characters. The default is “”.

location=*string*

The location of this device. The maximum length is 64 characters. The default is “”.

contact=*string*

The contact for this device. The maximum length is 64 characters. The default is “”.

Example

Set description, contact, and location

```
#> set system description=”Engineering printer”
location=”Room 1347” contact=”John Doe at x-3749”
```

See also

- "revert"
- "show"

set tcpserial

Purpose

Configures behaviors of TCP serial connections and displays current TCP serial settings. This command affects the following TCP serial connections:

- Connections made using the autoconnect feature.
- Incoming network connections made to the following:
  - The TCP server (raw socket, IP port 2101~2132 by default)
  - The Telnet server (telnet socket, IP port 2001~2032 by default)
  - The SSH server (telnet socket, IP port 2501~2532 by default)
  - Secure Sockets Layer (ssl socket, IP port 2601~2632 by default)
- Default IP port number can be changed using “set service” command

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the TCP serial settings for the line on which they are logged in: “set permissions s-tcpserial=r-self”
- For a user to display the TCP serial settings for any line:
- “set permissions s-tcpserial=read”
- For a user to display and set the TCP serial settings for the line on which they are logged in: “set permissions s-tcpserial=rw-self”
- For a user to display the TCP serial settings for any line, and set TCP serial settings for the line on which the user is logged in:
- “set permissions s-tcpserial=w-self-r”
- For a user to display and set the TCP serial settings on any line:
- “set permissions s-tcpserial=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Set behaviors of TCP serial connections

```
set tcpserial port=range
  [hangupdcd={on|off}]
  [hangupdsr={on|off}]
  [idletime={0|n}]
  [sid={on|off}]
  [sidstring=socketid string]
  [buffered={on|off}]
  [sendcount=1-65535] (bytes)
  [sendtime={0|1-65535}] (milliseconds)
  [endpattern=string]
  [strippattern={on|off}
```

Display TCP serial settings

```
set tcpserial [port=range]
```

Options

port=*range*

Used to specify the serial port. Optional on a single-port device. To configure settings for an XBee port, specify "port=xbee." To configure settings for an internal modem port, specify "port=internalmodem."

hangupdcd={on|off}

Indicates whether an established network connection should be terminated when the serial port's DCD signal drops. The default is "off."

hangupdsr={on|off|}

Indicates whether an established network connection should be terminated when the serial port's DSR signal drops. The default is "off."

idletime=idletime={0|n}

Indicates that established network connection should be terminated if the serial port is idle for the specified amount of time in seconds. A value of 0 (zero) disables this option. The default is 0.

sid={on|off}

Determines how the socket ID (SID) string in the “sidstring” option is handled.

on

The value for the “sidstring” option is sent to the network destination right before the first data bytes are sent to the network.

off

The value for the “sidstring” option is not sent to the network destination.

The default is "off."

sidstring=*socketid string*

When the “sid” option is set to on, this string is sent to the network destination right before the first data bytes are sent to the network. The maximum length of this string is 32 characters, including escape sequences for special characters. The maximum parsed length of this string is 32 characters. That is, this string must reduce down to a 32-character string when the escape sequences are processed. For more details on the escape sequences, see "Entering Special Characters in String Values".

buffered={on|off}

Turning on this feature on allows controlling how serial data is sent out to the network. The “sendcount,” “sendtime,” “endpattern,” and “strippattern” options are used to control how data is sent out once the “buffered” option is set to “on.” The default is “off.”

sendcount=1-65535 (bytes)

Indicates that data from the serial port should be sent out to the network after buffering the given number of bytes. This option only is valid when the “buffered” option is “on.” The default is 1024 bytes.

sendtime={0|1-65535} (milliseconds)

Indicates that data from the serial port should be sent out to the network after the given amount of time has passed where no new data has arrived from the serial port. This option only is valid when the “buffered” option is “on.” A value of 0 (zero) disables this option. The default is 0.

endpattern=*string*

Indicates that data from the serial port should be sent out to the network after the given endpattern string has been found in the data from the serial port. This option only is valid when the “buffered” option is “on.” An empty string disables this option.

The maximum length of this string is 32 characters, including escape sequences for special characters. For more details on the escape sequences, see "Entering Special Characters in String Values”. The maximum parsed length of this string is 4 characters. That is, this string must reduce down to a 4-character string when the escape sequences are processed.

strippattern={on|off}

This option corresponds with the “endpattern” option. When a valid “endpattern” string is found, this option indicates whether the matching string is stripped or kept in the data stream. The default is “off.”

Examples

```
#> set tcpserial hangupdcd=off idletime=20

#> set tcpserial port=1 sid=on sidstring=”abc”
#> set tcpserial port=1 buffered=on sendtime=50
sendcount=512
#> set tcpserial
```

See also

- "revert"
- "show"

set time

Purpose

Set system time or display current system time.

Sets the Coordinated Universal Time (UTC) and/or system time and date on the ConnectPort LTS device. If the “offset” option is set to anything other than “00”, this command assumes that if date and time are being set, they are system time. Out of the box, all ConnectPort LTS devices maintain time and date as the UNIX epoch (00:00:00, January 1, 1970) plus device up-time. Date and time will revert to the UNIX epoch on each reboot or power-cycle. Device time can be set manually using the web or command-line interfaces. The time and date are completely local to the device and have limited usefulness since they are not persistent over reboots/power-cycles. The “offset” option could be useful in adjusting for daylight savings time. Setting the date and time to standard time and setting “offset” to 1 whenever daylight savings time is in effect would serve that purpose. For users with several devices in different time zones, keeping “offset=0” might be useful for comparing logs or traces from different devices, since all would be using UTC.

Required permissions

Root privileges are required to set system time. Other users can only display the current system time.

Syntax

Set system time

```
set time={hh:mm:ss|hh:mm}
  date=mm.dd.yy
  offset={hh:mm|hh}
```

Display current system time

```
set time
```

Options

time={*hh*:*mm*:*ss*|*hh*:*mm*}

hh

Hour; ranges from 0 to23.

mm

Minute; ranges from 0 to 59.

ss

Second; ranges from 0 to 59.

date=*mm.dd.yy)*

mm

Month; ranges from 1 to12.

dd

Day; ranges from 1 to 31.

yy

Year; ranges from 0 to 99.

offset={*hh*:*mm*|*hh*}

hh

Hour offset; ranges from -12 to 14.

mm

Minute offset; allowed values are one of 00,15,30, or 45.

Examples

Set system time

```
#>set time=09:30:00 date=03.15.10
```

Display current time

```
#>set time
Time settings:
Current System Date and Time: Sun Mar 11 15:29:32
2001
```

set trace

Purpose

Configures a ConnectPort LTS product for tracing and displays tracing information.

Important: The **"**set trace**"** command should be used when working with Digi Technical Support. Enabling tracing can have an impact on system performance. Digi provides no guarantee that trace output is the same across firmware revisions.

Required permissions

For Digi products with two or more users, permissions must be set to "set permissions s-trace=read" to display tracing information, and to "set permissions s-trace=rw" to display tracing information and configure trace options. See "set permissions" for details on setting user permissions for commands.

Syntax

Display latest command options

The syntax and available options for "set trace" may vary by product and product release. Enter the following command to view the current list of options:

```
help set trace
```

Configure trace options

```
set trace [state={off|on|dump}]
  [mode={historical|concurrent}]
  [syslog={on|off}
  [loghost=ip address]
  [mask=type:severity]
```

Display tracing information

```
set trace
```

Options

state={off|on|dump}

Sets the state of the tracing function.

off

Turns the tracing function off.

on

Turns the tracing function on.

dump

Displays historical trace messages, when "mode" is set to "historical."

mode={historical|concurrent}

Sets handling of trace messages.

historical

All trace messages stored in the buffer will be displayed by issuing the command:

```
#> set trace state=dump
```

concurrent

All trace messages are printed to the administrative terminal.

syslog={on|off}

Enables or disables sending trace messages to the syslog server identified by the "loghost=*ip address*" option.

loghost=*ip address*

The IP address of a host to which trace messages should be sent. This host must be running the syslog daemon.

mask=*type*:*severity*

Identifies the type and nature of events that should be traced, and the severity level of the events.

type

The type of events that should be traced. Enter "set trace ?" to view the list of types supported in the ConnectPort LTS product. Some commonly used trace types for diagnosing connection problems are "modem" and "ppp." Contact Digi Technical Support for assistance in using the appropriate type keyword.

***severity*={assert|critical|warning|info|debug}**

The severity level of events traced.

assert

Tracing is done on assert lines only. This severity level is for Digi-internal use only.

critical

Tracing is done on only the most severe events. This is the default severity level. This level produces the least amount of trace data.

warning

Tracing is done on critical events and on less severe events as well. This level produces more trace data than "critical," but less than "info."

info

Tracing is done on many events. It produces more trace data than assert, critical, and warning levels.

debug

This severity level is used for Digi-internal debugging purposes only.

Examples

Display current trace settings

```
#> set trace
trace is currently off, using historical mode
syslog is currently off, loghost is ""
logfile is ""
  system    : _________    web       : _________    confmenu   : _________
  confhdlr  : _________    snmp      : _________    addp       : _________
  fwupd     : _________    xinetd    : _________    connect    : _________
  ppp       : _________    ssh       : _________    ssl        : _________
  pmodem    : _________    syschkr   : _________    serialp    : _________
```

Enable tracing and print all serial critical, info, and debug data to the screen

```
#> set trace state=on mode=concurrent mask=serialp:+cid
```

Enable tracing and send all ssh info and debug data to a syslog server.

```
#> set trace state=on syslog=on loghost=SYSLOG_IP mask=ssh:+id
```

Output Refer to Digi Technical Support for descriptions and interpretations of trace output. Digi provides no guarantee that trace output is the same across firmware revisions.

See also

- The “info” commands. These commands display various device statistics that may aid in troubleshooting.
- The *ConnectPort LTS User’s Guide*
- The Digi Support web page, to contact Technical Support, search Digi’s knowledge base, ask a question on the Support forum, and get diagnostics and utilities.

set udpserial

Purpose

Configures and displays current settings for the UDP serial feature. This feature allows data to be sent between the serial port and one or more remote network destinations using the UDP protocol. When this feature is enabled for a given serial port, data sent to the serial port will be sent out to the configured destinations. Also any time data is sent to the UDP serial service (IP port 2101) and the serial port is not being used by another service, the data will be sent to the serial port.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display the UDP serial settings for the line on which they are logged in: “set permissions s-udpserial=r-self”
- For a user to display the UDP serial settings for any line:
- “set permissions s-udpserial=read”
- For a user to display and set the UDP serial settings for the line on which they are logged in: “set permissions s-udpserial=rw-self”
- For a user to display the UDP serial settings for any line, and set UDP serial settings for the line on which the user is logged in:
- “set permissions s-udpserial=w-self-r”
- For a user to display and set the UDP serial settings on any line:
- “set permissions s-udpserial=rw”

See "set permissions" for details on setting user permissions for commands.

Syntax

Set general UDP serial forwarding characteristics for a serial port

```
set udpserial port={range|xbee|internalmodem}
  [state={on|off}]
  [sendcount=bytes]
  [sendtime={0|time}]
  [endpattern=string]
  [strippattern={on|off}]
  [sid={on|off}]
  [sidstring=string}
```

Set UDP destinations for a given serial port

```
set udpserial port=range
  range=1-64
  [active={on|off}
  [ipaddress=ip address}
  [ipport=ip port]
```

Display current UDP serial settings

```
set udpserial [port=range [range=range]]
```

Options

Options for setting general UDP serial forwarding characteristics

port=*range*

Used to specify the serial port. Optional on a single-port device. To configure settings for an XBee port, specify "port=xbee". To configure settings for an internal modem port, specify "port=internalmodem".

state={on|off}

Indicates whether an established network connection should be terminated when the serial port's DCD signal drops. The default is "off."

sendcount=*bytes*

The number of bytes received from the serial port that will cause the data to be sent on to the network destinations. This trigger cannot be disabled. The default is 1024 bytes.

sendtime={0|*time*}

The amount of idle time, in milliseconds, allowed before sending data to the network. If no data is received on the serial port for the time specified by this option, any buffered data will be sent on to the network destinations. A value of 0 (zero) disables this trigger.

endpattern=*string*

If this string is set, any pattern match of data received from the serial port will cause the data to be sent on to the network destinations. The maximum length of this string is 32 characters, including escape sequences for special characters. For more details on the escape sequences, see "Entering Special Characters in String Values". The maximum parsed length of this string is 4 characters. That is, this string must reduce down to a 4-character string when the escape sequences are processed.

strippattern={on|off}

Determines how the data specified by the “endpattern” option is handled.

on

The endpattern that is found is stripped from the stream before any data is to be sent on to the network destinations.

off

The endpattern is not stripped from the stream before data is sent on to network destinations.

The default is "off."

sid={on|off}

Determines how the socket ID (SID) string in the “sidstring” option is handled; that is, whether the string specified by the “sidstring” option is sent at the beginning of each UDP packet.

on

The value of “sidstring” is sent at the beginning of each UDP packet.

off

The value of “sidstring” is not sent at the beginning of each UDP packet.

The default is "off."

sidstring=*string*

The string sent at the beginning of each UDP packet if the “sid” option is set to on. The maximum length of this string is 32 characters, including escape sequences for special characters. For more details on the escape sequences, see "Entering Special Characters in String Values". The maximum parsed length of this string is 32 characters. That is, this string must reduce down to a 32-character string when the escape sequences are processed.

Options for setting UDP destinations for a given serial port

The following options require a range to be specified by the “range” option.

port=*range*

Specifies the serial port. Optional on a single-port device.

range={1-64}

Specifies the UDP destination to be configured.

active={on|off}

Specifies whether data from the serial port is sent to this destination.

on

Data from the serial port is sent to this destination.

off

This destination is not sent any data.

The default is “off.”

ipaddress=*ip address*

The IP address of the network destination to which data is sent.

ipport=*ip port*

The UDP port of the destination to which data is sent.

Options for displaying current UDP serial settings

port=*range*

Used to specify the serial port. Optional on a single-port device.

range=*range*

Identifies the range of UDP destinations to be displayed.

Examples

Set UDP destinations for a given serial port

In this example, data will be sent to the destination identified.

```
#> set udpserial port=1 range=1 ipaddress=10.0.0.1
ipport=2101 active=on
```

Display current UDP serial settings

The following are all valid ways of using set udpserial to display current UDP serial settings:

```
#> set udpserial
```

See also

- "revert"
- "show"

set usb

Purpose Configure USB device settings and displays current USB settings.

Required permissions Permissions must be set to one of the following:

- For a user to display the USB settings: “set permissions s-usb=read”
- For a user to display and set the SD memory settings: “set permissions s-usb=rw”

Syntax

Configure USB device settings

```
set usb
  [id=device id number]
  [state={off|on}
  [format]
  [fstype={ext2|vfat}]
```

Configure USB Modem options

These options configure a USB dongle cellular modem.

```
set usb
  [apn=string]
  [pin=string]
  [number=string]
  [auth={none|chap|pap|both}]
  [user=string]
  [password=string]
```

Display USB information

```
set usb
```

Options

id=*usb port number*

Specifies the USB port number to be set.

state={on|off}

Specifies whether the USB device will be enabled.

on

Enable the USB device.

off

Disable the USB device.

format

Format the device, using a default file system type of **ext2**. To format with an alternate file system type, use the "fstype" option.

fstype={ext2|vfat}

The file system type.

ext2

ext2 or second extended filesystem.

vfat

Virtual file allocation table filesystem.

USB Modem options

Obtain the values for these options from your cellular service provider.

apn=*string*

The Access Point Name (APN).

pin=*string*

The pin for logging on the USB modem.

number=*string*

The dial-in number for logging onto the cellular network for the USB modem.

auth={none|chap|pap|both}

The authentication protocol for connections over the USB modem.

none

The remote user does not require authentication.

chap

Challenge Handshake Authentication Protocol (CHAP) authentication is required.

Note: MS-CHAP is not supported.

pap

Password Authentication Protocol (PAP) authentication is required.

both

Both CHAP and PAP authentication are required.

The default is “none.” CHAP authentication works between two Digi Connect products. CHAP will be negotiated to PAP for all other connections.

user=*string*

The user name for logging onto the cellular network via the USB modem.

password=*string*

The password for logging the specified username onto the cellular network via the USB modem.

Example **Format the USB memory**

```
#>set usb format id=1
```

See also "show usb"

set user

Purpose

Used to:

- Add users for access to a ConnectPort LTS product. Up to 32 users can be defined.
- Associate a user with up to two groups. A user can be associated with up to two groups.
- Disassociate a user from a group.
- Remove users.
- Change user settings.
- Display user settings.
- Load an SSH public key.

Required permissions

For products with two or more users, to use this command, permissions must be set to one of the following:

- For a user to display user configuration attributes: "set permissions s-user=read"
- For a user to display and set user configuration attributes: "set permissions s-user=rw"

See "set permissions" for details on setting user permissions for commands.

Default permissions for a new user

When a new user is created, it is given a set of default permissions. Once a user is created, an administrator can adjust permissions up or down as needed. Default permissions for a new user are as follows. For more information on user permissions, see "set permissions."

- **none**: backup, boot, buffers, connect, display, filesys, kill, revert-all, s-alarm, s-pmodem, s-snmp, status, s-trace, s-profile, ping, python, s-internalmodem,s-lcd, s-modem, s-ppp, s-portauth, s-python, s-serial, s-sdmemory, s-sysauth, s-socket_tunnel, s-term, s-usb, s-xbee, webui
- **execute**: reconnect, rlogin, telnet, who
- **read**: s-host, s-permissions, s-ethernet, s-group, s-network, s-serial, s-service, s-system, s-user
- **r-self:** s-autoconnect, s-rtstoggle, s-tcpserial, s-udpserial
- **rw-self:** newpass

Syntax

Add a user

```
set user add id=number name=user name
  [commandline={on|off}]
  [groupaccess={on|off}]
  [defaultaccess={commandline|group|none}]
  [defaultgroup={none|index|name of group for default
  access)
  [public_key=tftphost:filename]
```

Remove a user

```
set user remove {id=1-32|name=user name}
```

Associate a user with a group

```
set user associate {id=number|name=user name}
{gid=group id|gname=string}
```

Disassociate a user from a group

```
set user disassociate {id=number|name=user name}
{gid=number|gname=group name}
```

Change user settings

```
set user [id=1-32|name=user name]
  {gid=group id|gname=group name}
  [newname=new user name]
  [commandline={on|off}]
  [groupaccess={on|off}]
  [defaultaccess={commandline|group|none}]
  [defaultgroup={none|index|name of group for default
  access)
[public_key=tftphost:filename]
```

Display user settings

```
set user {id=range|name=string}
```

Display user settings for all users

```
set user
```

Load an SSH public key

```
set user public_key=tftphost:filename }
```

Remove an SSH public key

```
set user public_key=clear
```

Options

add

Add a user. New users are created with the default permissions (see "Default permissions for a new user" earlier in this description). A maximum of 32 users can be defined.

remove

Remove users.

associate

Associate a user with a group. A user can be associated with a maximum of two groups.

disassociate

Disassociate a user from a group.

id=1-32

Specifies the ID or range of IDs of the users to be acted on.

name=*user name*

Specifies the name of the user to be acted on.

newname=*new user name*

Specifies a new user name.

gid=*number*

Specifies the identifier for the group being associated with a user. If omitted, the "gname" option must be specified.

gname=*group name*

Specifies the name of the group being associated with a user. If omitted, the "gid" option must be specified.

commandline={on|off}

Specifies whether the user is allowed to access the command line of the device.

on

User can access the command line interface.

off

User can not access the command line interface.

The default is "on."

groupaccess={on|off}

Specifies whether the user is allowed to use the access rights for any associated groups. This allows a group to define the access rights for users. For instance, if the user has “commandline=off” and an associated group has “commandline=on,” then the user will have command line access if “groupaccess=on.”

on

The user can use group access rights.

off

The user cannot use group access rights.

The default is “off”

defaultaccess={none|climenu|shell}

Specifies the default access method to the ConnectPort LTS device, and the interface that a user will be given upon logging into the device. Note that the specified interface must be enabled for the user and have a valid menu and/or group if specified.

none

The user has no default access to the device and must explicitly specify the access type. If the user and/or associated group has no access rights then the user is not allowed to access either the command line interface or the Linux shell.

climenu

The user can display and access the command-line menu interface.

shell

The user will be displayed and given access to the Linux shell (Linux command line interface) assuming the user and/or associated groups have command line access rights enabled. The default is “off.”

The default for this option is “climenu.”

public_key={*tftphost*:*filename*|clear}

Loads or clears an SSH public key used for authentication of this user. The key must be an RSA or DSA public key, in either OpenSSH or the IETF draft format.

tftphost*:*filename

Loads an SSH2 public key for use with this user, where:

tftphost

The IP address or DNS name of a host from which the SSH public key will be downloaded to the ConnectPort LTS product using TFTP.

filename

The name of a file on the host that contains the SSH public key. If your host's implementation requires a complete path to this file, specify the path here as well.

clear

Unloads an SSH public key.

Examples

Add a new user

```
#> set user add newname=jsmith id=4
```

Remove user 7

```
#> set user remove id=7
```

Associate user “johndoe” with the root group

```
#> set user associate name=johndoe gname=root
```

Disassociate user 15 from group 2

```
#> set user disassociate id=15 gid=2
```

Set a new user name to be entered at login

```
#> set user id=4 newname=jdoe
```

Set a user to have default command line interface access

```
#> set user id=4 defaultaccess=commandline
```

See also

- "newpass"
- "revert"
- "set group"
- "set permissions"
- "show"
- "newpass"

- “User permissions in ConnectPort LTS products” on page 13.

set web

Purpose Configure the timeout value for the web interface.

Required permissions Permissions must be set to one of the following:

- For a user to display the Web server settings:
  "set permissions s-service=read"
- For a user to display and set the Web server settings:
  "set permissions s-service=rw"

Syntax **Set time-out value for Web server**

```
set web [timeout=0-1140]
```

Display Web server settings

```
set web
```

Options **timeout=0-1140**

Specifies the time-out value in minute for Web server login.
If there is no user input during time-out, user will be logged out from Web server automatically. Setting the timeout to 0 means that user will not be logged out once logged in.

Example

```
#>set web timeout=60
```

See also "show web"

set xbee

Purpose

The “set xbee” command performs several functions:

- Displays current configuration settings for the XBee RF module
- Displays Xbee settings for a particular node
- Changes the state of the XBee RF module (enabled/disabled)
- Loads firmware to the XBee RF module
- Executes AT commands on the XBee RF module

The XBee RF module is regarded as one of the serial ports on the ConnectPort LTS device. To configure other non-XBee settings for access to the XBee RF module, please see the commands related with serial ports, such as "set serial", "set tcpserial", "set udpserial", "set portauth", “set service" and "set autoconnect."

Required permissions

Permissions must be set to one of the following:

- For a user to display the Xbee settings: “set permissions s-xbee=read”
- For a user to display and set the Xbee settings: “set permissions s-xbee=rw”

Syntax

Display current configuration settings for the XBee RF module

```
set xbee
```

Display Xbee settings for a particular node

```
set xbee address={id|address}
```

Change XBee RF module state

```
set xbee state={on|off}
```

Load firmware to the XBee RF module

```
set xbee load={host:filename}
```

Execute an AT command on the XBee RF module

```
set xbee <CC>[[=]param]
```

Options **state={on|off}**

on

The XBee RF module can be managed from the command-line interface. That is, you can issue AT commands to the XBee RF module from the command-line interface.

off

Release exclusive mode.

The XBee RF module cannot be managed via the command-line interface. AT commands cannot be issued the XBee RF module via the CL. However, the XBee RF module can be accessed via a network service such as Telnet.

The default is “off.”

load={*host*:*filename*}

Loads firmware to the Xbee module.

host

The IP address of a host with new firmware. The host must be running a TFTP server.

filename

The name of a firmware file.

address=(*id*|*address*}

Specify Xbee module using one of these value types:

id

The ID number of the Xbee module.

address

The name of a firmware file.

<*CC*>[[=]*param*]

Run an AT command on the XBee RF module. Supported AT commands include: AI, AR, BH, CH, DD, DB, EA, EE, EO, HV, ID, II, KY, LT, MP, NC, NP, NJ, NH, NK, NI, NT, MY, OI, OP, PL, PM, SC, SD, SH, SL, SM, SN, SO, SP, ST, VR, ZS. D5 is not supported.

CC

A 2 character AT command, entered in uppercase.

param

Parameters for the AT command. Parameter values can be of type <decimal>, 0x<hex>, or "string."

Examples

Set Xbee state ON (Exclusive mode is turned on)

```
#>set xbee state=on
```

Run the AT command “NI”

```
#>set xbee NI
```

Change the XBee ID using the AT command “ID”

```
#> set xbee ID=0x001002F04
```

See also

- "show xbee"
- "set serial"
- "set tcpserial"
- "set udpserial"
- "set portauth"
- "set service"
- "set autoconnect"

show

Purpose

Displays the current settings in a device, including current configuration settings, boot code loaded in the device, and the effects of commands issued to the device.

Required permissions

For products with two or more users, for this command to display current device settings, the various “set” commands must have be set to either “read” or “r-self,” depending on the available permissions for the commands. See "set permissions" for details on setting user permissions for commands.

Syntax

`show` *`option`* `[port=`*`range`*`] [range=`*`range`*`]`

Options

option

Specifies which settings in the device to show. The following options can be specified. The use of the “port” and “range” options on the show command depends on whether the command that was used to configure the settings uses the “port” and “range” options as well.

Option	Displays settings configured by	Works w/port option	Works w/range option
alarm	set alarm	No	Yes
autoconnect	set autoconnect	Yes	No
buffer	set buffer	Yes	No
ethernet	set ethernet	No	No
group	set group	No	No
host	set host	No	No
permissions	set permissions	No	No
pmodem	set pmodem	Yes	No
profile	set profile	Yes	No
python	set python	No	Yes
realport	set realport	No	No
rtstoggle	set rtstoggle	Yes	No
serial	set serial	Yes	No
service	set service	No	Yes
snmp	set snmp	No	No
socket_tunnel	set socket_tunnel	No	No
system	set system	No	No
tcpserial	set tcpserial	Yes	No
udpserial	set udpserial	Yes	Yes (when specifying UDP serial destinations)
user	set user	No	Yes
ippool	set ippool	Yes	No
lcd	set lcd	No	No
modem	set modem	Yes	No

Option	Displays settings configured by	Works w/port option	Works w/range option
nfs	set nfs	No	No
portauth	set portauth	Yes	No
portgroup	set portgroup	No	Yes
ppp	set ppp	No	Yes
samba	set samba	No	No
sdmemory	set sdmemory	No	No
smtp	set smtp	No	No
switches	set switches	Yes	No
sysauth	set sysauth	No	Yes
syslog	set syslog	No	Yes
time	set time	No	No
trace	set trace	No	No
usb	set usb	No	No
web	set web	No	No
xbee	set xbee	No	No

port=*range*

Identifies a particular serial port. Optional on a single-port device.

range=*range*

A configuration table entry or range of entries.

Examples **Display network configuration settings**

```
#> show network
Network configuration
 "eth0" interface configuration
  MAC address      :   00:04:9F:EF:23:33
  IPv6 Link addr   :   fe80::204:9fff:feef:2333/64
  IPv6 Site addr   :
  IPv6 Global addr  :   (Currently in use)

                     Currently in use by
                     the network stack        Stored configuration
                     -----------------------   -----------------------
IPv4 options
  mode_v4          :   static                 static
  ip_v4            :   192.168.4.47           192.168.4.47
  submask_v4       :   255.255.0.0            255.255.0.0
  gateway_v4       :   192.168.1.1            192.168.1.1

IPv6 options
  mode_v6          :   none                   none
  ip_v6            :   <none> (Stored configuration)
  gateway_v6       :   <none> (Stored configuration)
  ip_6to4tunnel    :   off                    off
  ip_v4_6to4relay  :   192.88.99.1            192.88.99.1
  ip_v6_v4addr     :   <none>                 <none>
```

```
 "eth1" interface configuration
  MAC address      :   00:E0:0C:00:7E:21
  IPv6 Link addr    :
  IPv6 Site addr    :
  IPv6 Global addr  :    (Currently in use)

                     Currently in use by
                     the network stack        Stored configuration
                     -----------------------   -----------------------
IPv4 options
  mode_v4          :   none                    none
  ip_v4            :                          <none>
  submask_v4       :                           <none>
  gateway_v4       :                           <none>

IPv6 options
  mode_v6          :   none                    none
  ip_v6            :   <none> (Stored configuration)
  gateway_v6       :    <none> (Stored configuration)
  ip_6to4tunnel    :    off                     off
  ip_v4_6to4relay  :    192.88.99.1              192.88.99.1
  ip_v6_v4addr     :    <none>                   <none>

General options
  manual_dns       :    off                     off
  dns1             :   206.13.28.12             0.0.0.0
  dns2             :   0.0.0.0                 0.0.0.0
  idle             :   7200                    7200
  probe_count      :    9                       9
  probe_interval   :    75                       75
  reuse_old_ip     :    off                      off
  autoip           :   off                     off
```

Display current alarm settings

```
#> show alarm
```

Display settings for a particular user

```
#> show user range=3
```

See also

• "revert"

• The “set” commands (“set user,” “set network,” “set serial,” etc.). Entering a set command without any options displays the same information as that displayed by the “show” command.

status

Purpose

Displays the current list of sessions. The “status” command displays the status of outgoing connections (connections made by “connect,” “rlogin,” or “telnet” commands). In contrast, the “display” command displays real-time information about a device, while the “info” command displays statistical information about a device over time. Typically, the “status” command is used to determine which sessions to close.

Required permissions

For products with two or more users, permissions must be set to “set permissions status=read” or “set permissions status=rw” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

```
status
```

Example

```
#> status
Connection: 3         From: 10.8.109.8
Connection not associated with any sessions.
```

See also

- "connect"
- "close", for information on ending a connection.
- "display"
- "info"
- "rlogin"
- "telnet"
- "who"

telnet

Purpose

Used to make an outgoing Telnet connection, also known as a session.

Required permissions

For products with two or more users, permissions must be set to "set permissions telnet=execute" to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax

`telnet` *`ipaddress`* [*`tcp port`*]

Options

ipaddress

The IP address of the host to which you want make a Telnet connection.

tcp port

The TCP port assigned the Telnet application on the remote system. The default is 23, the port typically used for Telnet.

Examples

Establish a Telnet session using an IP Address

In this example, the telnet command establishes a Telnet session using an IP address. The default TCP port (23) is used.

```
#> telnet 192.192.150.28
```

Establish a Telnet session to a device server port from the LAN

In this example, a user on the LAN initiates a Telnet connection to port 4 on a device server.

```
#> telnet 192.192.150.28 2004
```

See also

- "rlogin"
- "connect"
- "close"
- "status"

wan

Purpose

Initiates and controls wide-area network (WAN) connections, or displays the status of current WAN connections.

Required permissions

Anyone can display the status of WAN connections. Root privileges are required to initiate or control WAN connections.

Syntax

Initiate and control WAN connections

```
wan [close=username]
  [start=username]
  [range=range]
```

Display status of WAN connections

```
wan [range=range]
```

Options

close=*username*

Closes the specified WAN interface

start=*username*

S the specified WAN interface

range=*range*

The range of ports to which the command applies. This range begins with 0, which is the internal modem, or, if there is no internal modem, with the first serial port.

who

Purpose Displays active connections to and from the device.

Required permissions For products with two or more users, permissions must be set to “set permissions who=execute” to use this command. See "set permissions" for details on setting user permissions for commands.

Syntax `who`

Options None at this time.

Example **Display a list of all current connections**

```
#> who
ID User name      From                       To            Protocol
-- -------------- -------------------------- ------------ --------------------
 1 root           10.8.16.115                local host    telnet
 2 root           ::ffff:10.4.102.1          webui         http
```

See also • "kill." The “kill” command is used to kill a connection.